

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-288448

(43)Date of publication of application : 04.10.2002

(51)Int.Cl. G06F 17/60

G06K 17/00

G06K 19/07

(21)Application number : 2001-087395 (71)Applicant : SANYO ELECTRIC CO LTD

(22)Date of filing : 26.03.2001 (72)Inventor : HORI YOSHIHIRO
YOSHIKAWA TAKATOSHI

(54) LICENSE RECORDER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a license recorder which provides a backup of a leased license.

SOLUTION: A memory card 1 is provided with a license area 1415A. The license area 1415A includes licenses (a license ID, a contents ID, a license key Kc, access control information Acm, and reproducing frequency control information Acp), a validity flag, a lease flag, a leased party ID, and license ID at the time of lease. When the license is leased 'under lease' is set to the lease flag, and a public cipher key peculiar to a memory card of the leased party is stored in the leased party ID, and the license ID for lease is stored in the license ID at the time of lease.

LEGAL STATUS [Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

*** NOTICES ***

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.*** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] It is the license recording device which generates the license for a loan from the license for decoding encryption contents data, and lends out said license for a loan to other license recording devices. Said license, The loan flag which shows the loan propriety of said license, and the loan place specific information for specifying the loan place of said license for a loan, It has a license attaching part holding the license identification information for a loan for identifying said license for a loan, and a control section. Said control section The license specific information for a loan for specifying the license assignment information for specifying the license set as the object of the loan to a license recording device and said license for a loan is received from the exterior. a loan demand of said license -- responding -- said -- others -- The license specified using said license assignment information From said license attaching part to read-out The license recording device which replaces the license specific information for being contained in the read license and specifying the license which carried out [aforementioned] read-out with said license specific information for a loan, generates said license for a loan, and is set up while lending out said loan flag.

[Claim 2] Said control section is a license recording device according to claim 1 which generates said license for a loan when the license read from said license attaching part is a license to which the duplicate was forbidden to and migration was permitted.

[Claim 3] Said control section is a license recording device according to claim 1 or 2 which generates said license for a loan when it is shown that said loan flag is not lending out said license.

[Claim 4] said control section -- further -- said -- others -- the license recording device of the publication by any 1 term of claim 1 to claim 3 generate the control information for forbidding the migration and the duplicate of said license for a loan in a license recording device, replace with the control information which it was contained in the license read from said license attaching part, and forbade in the duplicate of the license which carried out [aforementioned] read-out to said control information which generated, and generate said license for a loan.

[Claim 5] Said control section is a license recording device given in any 1 term of claim 1 to claim 4 further stored in said license attaching part by making said license specific information for a loan into said license identification information for a loan.

[Claim 6] said control section -- further -- said -- others -- a open cryptographic key peculiar to a license recording device -- said -- others -- a license recording device given in any 1 term of claim 1 to claim 5 which receives from a license recording device and is stored in said license attaching part by making the open cryptographic key which received into said loan place specific information.

[Claim 7] It is a license recording device given in any 1 term of claim 1 to claim 6 in which said license attaching part stores said license, said loan flag, said loan place specific

information, and said license identification information for a loan in corresponding to the entry number which specifies a field, and said control section receives said entry number from the exterior as said license assignment information.

[Claim 8] Said license attaching part is a license recording device given in any 1 term of claim 1 to claim 7 which holds said loan place specific information and said license identification information for a loan according to the number of the loan places of a license.

[Claim 9] A license recording device given in any 1 term of claim 1 to claim 8 further equipped with the data storage section which records the encryption contents data reproduced by said license.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the license recording device which lends out the license for decoding and reproducing the encryption data acquired using the data distribution system which makes possible the protection of copyrights to the copied information to other license recording devices.

[0002]

[Description of the Prior Art] It is possible for each user to access an information communication network easily with the terminal for individuals using a portable telephone etc., and to acquire the data on an information communication network by the advance of information communication networks, such as the Internet, etc., in recent years.

[0003] In such an information communication network, information is transmitted by the digital signal. It is possible to perform a copy of data, without producing most degradation of the tone quality by such copy, or image quality, even when an each people user copies the music and image data which followed, for example, were transmitted in the above information communication networks.

[0004] Therefore, if the policy for suitable protection of copyrights is not taken when the contents data which are the creation object of authors, such as music data and image data, are transmitted on such an information communication network, there is a possibility of infringing on a copyright person's right remarkably.

[0005] On the other hand, top priority is given to the purpose of protection of copyrights, and supposing it cannot distribute contents data through the information communication network which carries out sudden expansion size, it will become rather disadvantageous also for the copyright person who can collect a fixed royalty on the occasion of the duplicate of work data fundamentally.

[0006] Here, about CD (compact disk) which recorded the music data usually sold, if it thinks and sees not taking the case of distribution through the above information communication networks but taking the case of the record medium which recorded the digital data, the music copy of data from CD to magneto-optic disks (MD etc.) can be freely performed in principle, as long as the copied music concerned is stopped to individual use. However, the individual user who performs digital sound recording etc. is to pay indirectly the fixed amount of the price of media, such as the digital sound recorder machine itself and MD, as a deposit to a copyright person.

[0007] And in view of such information being digital data which do not almost have copy degradation, when the music data which are a digital signal are copied to MD from CD, for protection of copyrights, copying music information to MD of further others as digital data from recordable MD could not do a device constitutionally, and it is come.

[0008] Since distributing music data and image data to the public through an information

communication network also from such a situation is an action from which itself receives the limit by a copyright person's public transmission right, sufficient policy for protection of copyrights needs to be devised.

[0009] In this case, it is necessary for the contents data received once to prevent being reproduced still more freely about contents data transmitted to the public through an information communication network, such as music data and image data.

[0010] Then, the data distribution system by which the distribution server holding the encryption contents data which enciphered contents data distributes encryption contents data through a terminal unit to the memory card with which terminal units, such as a portable telephone, were equipped is proposed. In this data distribution system, it transmits to a distribution server in the case of the distribution demand of the open cryptographic key and certificate of the memory card beforehand attested by the certificate authority of encryption contents data, and the license key for decoding encryption contents data and encryption contents data to a memory card, after checking having received the certificate with which the distribution server was attested is transmitted. And in case encryption contents data and a license key are distributed, a distribution server and a memory card generate a different session key for every distribution, by the generated session key, encipher a open cryptographic key and exchange keys a distribution server and between memory cards.

[0011] Finally, a distribution server transmits the license which it was enciphered by the open cryptographic key of memory card each, and was further enciphered by the session key, and encryption contents data to a memory card. And a memory card records the license key and encryption contents data which were received on a memory card.

[0012] And a cellular phone is equipped with a memory card when reproducing the encryption contents data recorded on the memory card. A cellular phone also has a specialized circuit for decoding the encryption contents data from a memory card other than the usual telephone function, and reproducing, and outputting to the exterior.

[0013] Thus, the user of a portable telephone can receive encryption contents data from a distribution server using a portable telephone, and can reproduce the encryption contents data.

[0014] On the other hand, distributing encryption contents data to a personal computer using the Internet is also performed. And in distribution of the encryption contents data to a personal computer, distribution of encryption contents data is performed by the software installed in the personal computer, and the security to encryption contents data is lower than the case where encryption contents data are written in a memory card. Moreover, if a personal computer is equipped with a device with the same security as the above-mentioned memory card, it is possible to perform the same distribution as the distribution of encryption contents data to the above-mentioned portable telephone to a personal computer.

[0015] If it does so, a personal computer will receive encryption contents data with the

installed software and the above-mentioned device. That is, a personal computer receives the encryption contents data with which security level differs.

[0016] Furthermore, the music CD on which music data were recorded has spread widely, and acquiring music data from this music CD by ripping is also performed. And the license for decoding encryption music data (encryption contents data) and its encryption music data, and reproducing from music data, by this ripping, is generated. And in this ripping, the water mark which makes the use regulation of contents data is detected from contents data, and encryption contents data and a license are generated according to the contents of that detected water mark.

[0017] As mentioned above, a portable telephone and a personal computer receive the encryption contents data and the license which were enciphered from the distribution server. And the user of a portable telephone and a personal computer may move or reproduce the encryption contents data and the license which were received to other portable telephones or personal computers of a user. In this case, as for a user, it is free to move / reproduce encryption contents data to other portable telephones or personal computers of a user, and he cannot move freely the license with which ** decodes encryption contents data to other portable telephones or personal computers of a user. That is, a license is controlled according to the conditions which the contents feeder defined, and although the license and duplicate which can reproduce freely are forbidden, the license to which migration is permitted, and the license which forbids both a duplicate and migration exist. Moreover, it is usually necessary to forbid a duplicate and migration from a viewpoint of protection of copyrights in ripping from Music CD. When it moves to other portable telephones or personal computers of a user, it cannot leave a license to both a transmitting side and a receiving side from a viewpoint of the protection of copyrights of encryption contents data. Then, when a license is moved, the license of a transmitting side is eliminated.

[0018] Moreover, to the license to which migration and a duplicate were forbidden, lending out a license to other memory cards etc. a condition [return] is performed.

[0019]

[Problem(s) to be Solved by the Invention] However, in the loan of the conventional license, the lent-out license and the license in a lending out agency cannot be matched with 1 to 1, and it cannot manage to a lending out agency. That is, there was a problem that backup of the license lent out to the lending out agency could not be offered.

[0020] Then, it is made in order that this invention may solve this problem, and the purpose is offering the license recording device which can offer backup of the lent-out license.

[0021]

[Means for Solving the Problem] According to this invention, a license recording apparatus generates the license for a loan from the license for decoding encryption contents data. It is the license recording device which lends out the license for a loan to other license recording

devices. A license, The loan flag which shows the loan propriety of a license, and the loan place specific information for specifying the loan place of the license for a loan, It has a license attaching part holding the license identification information for a loan for identifying the license for a loan, and a control section. A control section The license specific information for a loan for specifying the license assignment information for specifying the license set as the object of the loan to other license recording devices according to a loan demand of a license and the license for a loan is received from the exterior. The license specified using license assignment information From a license attaching part to read-out The license specific information for specifying the license which it was contained in the read license, and was read is replaced with the license specific information for a loan, and the license for a loan is generated, and while lending out a loan flag, it sets up.

[0022] Preferably, a control section generates the license for a loan, when the license read from the license attaching part is a license to which the duplicate was forbidden to and migration was permitted.

[0023] Preferably, a control section generates the license for a loan, when it is shown that the loan flag is not lending out the license.

[0024] It replaces with to the control information which generated the control information which forbade the duplicate of the license which the control information for forbidding migration and the duplicate of the license for the desirable loan in the license recording device of further others [control section] was generated, and it was contained in the license read from the license attaching part, and was read, and the license for a loan is generated.

[0025] Preferably, a control section is further stored in a license attaching part by making license specific information for a loan into the license identification information for a loan.

[0026] Preferably, a control section receives a open cryptographic key peculiar to the license recording device of further others from other license recording devices, and stores it in a license attaching part by making the open cryptographic key which received into loan place specific information.

[0027] Preferably, the license attaching part stores a license, a loan flag, loan place specific information, and the license identification information for a loan corresponding to the entry number which specifies a field, and a control section receives an entry number from the exterior as license assignment information.

[0028] Preferably, a license attaching part holds loan place specific information and the license identification information for a loan according to the number of the loan places of a license.

[0029] Preferably, a license recording apparatus is further equipped with the data storage section which records the encryption contents data reproduced by license.

[0030]

[Embodiment of the Invention] It explains to a detail, referring to a drawing about the gestalt

of operation of this invention. In addition, the same sign is given to the same or a considerable part among drawing, and the explanation is not repeated.

[0031] Drawing 1 is a schematic diagram for explaining notionally the whole data distribution system configuration whose license recording apparatus by this invention acquires encryption contents data.

[0032] In addition, although explained taking the case of the data distribution structure of a system which distributes digital music data to each personal computer through the memory card 110 equipped with digital music data by a user's cellular phone through the cellular-phone network, or the Internet below When distributing the contents data as other works, for example, image data, dynamic-image data, etc., this invention can be applied without being limited in such a case, so that it may become clear by the following explanation.

[0033] With reference to drawing 1 , the distribution carrier 20 relays the distribution demand (distribution request) from a user obtained through the cellular-phone network of self to the distribution server 10. The distribution server 10 which manages the music data with which copyright exists [whether the memory card 110 with which a cellular-phone user's portable telephone 100 accessed in quest of data distribution was equipped has just authentication data, and] Namely, after performing authentication processing of whether to be the memory card of normal and enciphering music data (it is also called contents data below) with a predetermined cipher system to a just memory card The license containing the license key for decoding encryption contents data as information required for the cellular phone company which is the distribution carrier 20 for distributing data in order to reproduce such encryption contents data and encryption contents data is given.

[0034] The distribution carrier 20 distributes encryption contents data and a license through a cellular-phone network and a portable telephone 100 to the memory card 110 with which the portable telephone 100 which transmitted the distribution demand through the cellular-phone network of self was equipped.

[0035] In drawing 1 , it has the composition that a cellular-phone user's portable telephone 100 is equipped with the removable memory card 110, for example. A memory card 110 is given to the music playback section in a portable telephone 100 (not shown) after decoding the encryption performed in a receipt and the above-mentioned distribution in the encryption contents data received by the portable telephone 100.

[0036] furthermore -- for example, the head telephone 130 grade which the cellular-phone user connected to the portable telephone 100 -- minding -- such contents data -- "-- reproducing, " carrying out and hearing is possible.

[0037] It becomes a difficult configuration to play music in response to distribution of contents data first, by considering as such a configuration, from the distribution server 10, if a memory card 110 is not used.

[0038] And in the distribution carrier 20, it becomes easy that the distribution carrier 20

collects the royalty generated by carrying out counting of the frequency whenever it distributes the contents data for one music whenever a cellular-phone user receives contents data (download) with the phonecall charges of a portable telephone, then for a copyright person to secure a royalty.

[0039] Moreover, in drawing 1 , a personal computer 50 can receive distribution of the same security level as having received using the portable telephone 100 and the memory card 110 by having the license management device (hardware) equipped with the same function as the function in connection with license management of a memory card 110. And a personal computer 50 receives encryption contents data and a license from the distribution server 10 through the Internet network 30. At this time, a license is directly received and recorded in a license management device using the cryptocommunication way according to a predetermined procedure between the distribution server 10 and a license management device. Encryption contents data are recorded on HDD as it is. This license management device holds transmission and reception of a license, and the confidentiality of management in hard like a memory card 110, and its confidentiality is high.

[0040] Furthermore, in drawing 1 , a personal computer 50 generates the encryption contents data limited to local use from the music data acquired from the music (Compact Disk) CD 60 which recorded music data using the license administrative module, and the license for reproducing encryption contents data. It is equivalent to the action which acquires encryption contents data and a license from ripping, a call, and Music CD in this processing. About the detail of ripping, it mentions later.

[0041] Furthermore, a personal computer 50 can be transmitted and received with the memory card 110 which the USB (UniversalSerial Bus) cable 70 connected with the portable telephone 100, and was equipped with encryption contents data and a license by the portable telephone 100 with it.

[0042] Furthermore, in drawing 1 , a personal computer 50 will become reproducible [encryption contents data], if a personal computer is equipped with the contents regenerative circuit which has confidentiality by hardware. Moreover, it will become refreshable, if sufficient confidentiality is securable even if it is contents playback by software. The detailed explanation about the playback in a personal computer is omitted in order to simplify the explanation in this application.

[0043] Therefore, in the data distribution system shown in drawing 1 , a personal computer 50 acquires encryption contents data and a license from Music CD while receiving encryption contents data and a license from the distribution server 10 through the Internet network 30. Moreover, the memory card 110 with which the portable telephone 100 was equipped receives the encryption contents data and the license which the personal computer 50 acquired from the distribution server 10 or music CD 60 while receiving encryption contents data and a license from the distribution server 10 through a cellular-phone network. The user of a

portable telephone 100 becomes possible [acquiring encryption contents data and a license from Music CD] by minding a personal computer 50.

[0044] Furthermore, the memory card 110 with which the portable telephone 100 was equipped becomes possible [shunting the encryption contents data and the license which were received from the distribution server 10 through the cellular-phone network in a personal computer 50].

[0045] Drawing 2 shows the data distribution system at the time of using the playback terminal 102 which does not have the function to receive encryption contents data and a license from the distribution server 10 through a cellular-phone network. In the data distribution system shown in drawing 2 , the memory card 110 with which the playback terminal 102 was equipped receives the encryption contents data and the license which the personal computer 50 acquired from the distribution server 10 or music CD 60. Thus, when a personal computer 50 acquires encryption contents data and a license, the user of the playback terminal 102 without communication facility can also receive encryption contents data.

[0046] In a configuration as shown in drawing 1 and drawing 2 Being needed on a system, in order to make refreshable the contents data enciphered and distributed at the user side of a cellular phone or a personal computer It is a method for distributing the cryptographic key in a communication link to the 1st. Further to the 2nd It is the method itself which enciphers contents data to distribute, and is the configuration of realizing contents data protection for preventing further the unapproved copy of the contents data distributed to the 3rd in this way.

[0047] The recording apparatus and data playback terminal (the data playback terminal which can reproduce contents is also called the portable telephone or personal computer.) with which authentication and the check function of this invention of operation of as opposed to [in / especially in a gestalt / the time of distribution and generating of each reproductive session] the migration place of these contents data were enriched, and un-attesting or a decode key was torn the following -- being the same -- by preventing the output of the contents data to receive explains the configuration which strengthens the protection of copyrights of contents data.

[0048] In addition, suppose that the processing which transmits contents data to each portable telephone, each personal computer, etc. is called "distribution" from the distribution server 10 in the following explanation.

[0049] Drawing 3 is drawing explaining properties, such as data for the communication link used, and information, in the data distribution system shown in drawing 1 and drawing 2 .

[0050] First, the data distributed from the distribution server 10 are explained. Dc(s) are contents data, such as music data. Encryption which can decode the contents data Dc with the license key Kc is given. Encryption contents data {Dc} Kc to which encryption which can

be decoded with the license key Kc was given is distributed to the user of a cellular phone or a personal computer from the distribution server 10 in this format.

[0051] In addition, in the following, it shall be shown that a notation called {Y} X gave encryption which can be decoded with the decode key X for Data Y.

[0052] Furthermore, from the distribution server 10, additional information Dc-inf as plaintext information, such as copyright about contents data or server access relation, is distributed with encryption contents data. Moreover, the license ID which is Control Code for specifying the license key Kc, the license key from the distribution server 10, etc. as a license is exchanged between the distribution server 10 and a portable telephone 100 or between the distribution server 10 and a personal computer 50. Moreover, License ID is used also in order to specify the license by distribution, i.e., a license aiming at use on a local. In order to distinguish what is depended on distribution, and the thing of local use, it is the license ID of local use which starts in "0", and the head of License ID presupposes that it is a beginning [from other than "0"] thing the license ID by distribution. Furthermore, the content ID which is a code for identifying the contents data Dc as a license, Are generated based on the license purchase conditions AC including information determined by assignment from the intention side by the side of a contents feeder, and a user side, such as the number of licenses, and functional limitation. The playback control information ACp which is the access-control information ACm which is the information about the limit to access of the license in a recording apparatus (a memory card or license management device), and the control information about the playback in a data playback terminal exists. The access-control information ACm is control information which is in charge of outputting the license from a memory card and a license management device, or a license key outside, and, specifically, has the limit information about migration and the duplicate of the count (number which outputs a license key for playback) of refreshable, and a license, the security level of a license, etc. In order to reproduce, after a contents regenerative circuit receives a license key, the playback control information ACp is information which restricts playback, and has a playback term, a reproduction speed modification limit, playback range assignment (partial license), etc.

[0053] Henceforth, suppose that content ID, the license key Kc, License ID and the access-control information ACm, and the playback control information ACp are combined, and it is named a license generically.

[0054] moreover, the count of playback (0:playback improper --) which is the control information to which the access-control information ACm restricts the count of playback henceforth for simplification having a count of 1 - 254:refreshable, and no 255:limit, and migration / duplicate flag (1:migration duplicate good --) which restricts migration and the duplicate of a license 2: Using only migration as the dyadic eye of good and the ban on 3:migration duplicate, the playback control information ACp shall restrict only the playback term (UTCtime code) which is the control information which specifies a refreshable term.

[0055] In the gestalt of operation of this invention, the effective flag which shows effective and the invalid of the license held at the recording apparatus of a transmitting agency is employed in the migration/duplicate of a license to the recording apparatus of a reception place of a transmitting agency from a recording apparatus (a memory card or license management device). When this effective flag is effective, it means that it is possible to take out a license from a memory card to the exterior, and when an effective flag is invalid, it means that a license cannot be taken out from a memory card to the exterior.

[0056] Moreover, license ID applies at the time of the loan which is the identification information for identifying the loan place ID which is the information for specifying the loan flag and the loan place of a license which shows whether the license held at the recording device of a transmitting agency can lend out to other recording devices, and the lent-out license in a loan/return of the license to the recording device of a reception place of a transmitting agency from a recording device.

[0057] Drawing 4 is drawing explaining properties, such as data for the authentication used in the data distribution system shown in drawing 1 and drawing 2, and information.

[0058] The open cryptographic key K_{Ppy} of a proper is formed in a contents regenerative circuit, and the open cryptographic key K_{Pmw} of a proper is formed in a memory card and a license management device. And the open cryptographic keys K_{Ppy} and K_{Pmw} can be decoded with the secret decode key K_{mw} of a proper in a contents regenerative circuit, respectively to the secret decode key K_{py} of a proper and a memory card, and a license management device. These public presentation cryptographic key and a secret decode key have a contents regenerative circuit, a memory card, and a different value for every class of license management device. These open cryptographic keys and a secret decode key are named generically, a class key is called, and the unit which shares a class public presentation cryptographic key for these open cryptographic keys, and shares a class secret decode key and a class key for a secret decode key is called a class. A class changes with the class of a manufacturing company or product, lots at the time of manufacture, etc.

[0059] Moreover, C_{py} is prepared as a class certificate of a contents regenerative circuit (a portable telephone, playback terminal), and C_{mw} is prepared as a memory card, a license management device, and a class certificate of a license administrative module. These class certificates have a contents regenerative circuit, a memory card, and different information for every class of a license management device. The Tampa-proof module is torn, or the code with a class key was broken, namely, the class which the secret decode key revealed is set as the prohibition object of license acquisition.

[0060] The class public presentation cryptographic key and class certificate of a memory card and a license management device are recorded [in the form of authentication data {K_{Ppy}//C_{py}} K_{Pa} / in the form of authentication data {K_{Pmw}//C_{mw}} K_{Pa}] for the class public presentation cryptographic key and class certificate of these contents regenerative circuits on

a data regenerative circuit, a memory card, and a license management device, respectively at the time of shipment. Although the back is explained to a detail, KPa is a open authentication key common to the whole distribution system.

[0061] Moreover, the secret decode key Kmcx of a proper exists in each which can decode the data enciphered by the open cryptographic key KPmcx set up for every medium and the open cryptographic key KPmcx which are called a memory card and a license management device as a key for managing data processing of a memory card 110 and a license management device. An individual open cryptographic key and a secret decode key are named generically for every memory card of this, an individual key is called, and an individual public presentation cryptographic key and the secret decode key Kmcx are called an individual secret decode key for the open cryptographic key KPmcx.

[0062] It is with a memory card, or as a cryptographic key for the nondisclosure in the data transfer to a license management device, whenever distribution of a license and playback are performed, the common keys Ks1-Ks3 generated in the distribution server 10, a portable telephone 100, a memory card 110, and a license management device are used.

[0063] here, the common keys Ks1-Ks3 are the unit of the communication link between a distribution server, a contents regenerative circuit, a memory card, a license management device, or a license administrative module, or the unit of access -- "-- it is the common key of a proper generated in every session", and suppose that these common keys Ks1-Ks3 are also called a "session key" to below.

[0064] These session keys Ks1-Ks3 are managed by having the value of a proper for every session by the distribution server, the contents regenerative circuit, the memory card, and the license management device. Specifically, the session key Ks1 is generated for every distribution session by the distribution server. The session key Ks2 is generated for every session in all sessions with a memory card and a license management device, and the session key Ks3 is generated for every playback session in a contents regenerative circuit. In each session, the security reinforcement in a session can be raised by delivering and receiving these session keys, and transmitting a license key etc. in response to the session key generated by other devices, after performing encryption by this session key.

[0065] Drawing 5 is the outline block diagram showing the configuration of the distribution server 10 shown in drawing 1 and drawing 2 .

[0066] The information database 304 for the distribution server 10 to hold delivery information which enciphered contents data according to the predetermined method, such as data and content ID, The accounting database 302 for holding the accounting information which followed the access initiation to contents data for every user of a cellular phone or a personal computer, The menu database 307 holding the menu of the contents data held at the information database 304, The distribution record database 308 holding the log about distribution of the transaction ID which specifies distribution of contents data, a license key,

etc. for every distribution of a license, The data-processing section 310 for performing a receipt and predetermined processing for the data from the information database 304, the accounting database 302, the menu database 307, and the distribution record database 308 through a bus BS 1, It has the communication device 350 for performing data transfer between the distribution carrier 20 and the data-processing section 310 through a communication network.

[0067] The distribution control section 315 for the data-processing section 310 to control actuation of the data-processing section 310 according to the data on a bus BS 1, The session key generating section 316 for being controlled by the distribution control section 315 and generating the session key Ks1 at the time of a distribution session, The authentication key attaching part 313 holding two kinds of open authentication keys KPa for decoding authentication data {K_{Pmw}//C_{mw}} KPa for the authentication sent from the memory card and the license management device, Authentication data {K_{Pmw}//C_{mw}} KPa for the authentication sent from the memory card, the license management device, and the license administrative module is received through a communication device 350 and a bus BS 1. The decode processing section 312 which performs decode processing with the open authentication keys KPa or KPb from the authentication key attaching part 313, The session key Ks1 generated from the session key generating section 316 and the session key generating section 316 which generate the session key Ks1 is enciphered using the class public presentation cryptographic key K_{Pmw} obtained by the decode processing section 312 for every distribution session. The encryption processing section 318 for outputting to a bus BS 1 and the decode processing section 320 which performs decode processing in response to the data transmitted after being enciphered by the session key Ks1 from a bus BS 1 are included.

[0068] The data-processing section 310 contains the encryption processing section 326 for enciphering further the license key Kc and the access-control information AC_m which are given from the distribution control section 315 by the individual public-presentation cryptographic key K_{Pmcx} of the memory card obtained by the decode processing section 320 and a license management device, and the encryption processing section 328 for enciphering further and outputting to a bus BS 1 by the session key Ks2 to which the output of the encryption processing section 326 is given from the decode processing section 320.

[0069] About the actuation in the distribution session of the distribution server 10, the back is explained to a detail using a flow chart.

[0070] Drawing 6 is an outline block diagram for explaining the configuration of the personal computer 50 shown in drawing 1 and drawing 2 . While a personal computer 50 controls the inside of the bus BS 2 for performing data transfer of each part of a personal computer 50, and a personal computer The controller 510 for performing various kinds of programs (CPU), The hard disk (HDD) 530 and CD-ROM drive 540 which are a mass recording apparatus for

connecting with a data bus BS 2 and a data bus BS 2, recording a program and data, and accumulating, The keyboard 560 for inputting the directions from a user and the display 570 for giving a user various kinds of information visually are included.

[0071] The USB interface 550 to control transfer of data between a controller 510 and a terminal 580 further, in case a personal computer 50 communicates encryption contents data and a license to portable telephone 100 grade, The terminal 580 for connecting the USB cable 70, and the modem 555 for controlling transfer of data between a controller 510 and a terminal 585, in case it communicates through the distribution server 10 and the Internet network 30, The terminal 585 for connecting with the Internet network 30 is included.

[0072] A controller 510 performs control at the time of acquiring encryption contents data and a license from Music CD by ripping through CD-ROM drive 540 while controlling transfer of data between the distribution servers 10, in order to acquire encryption contents data and a license from the distribution server 10 through the Internet network 30 by performing the license administrative module 511 which is a program. Furthermore, a personal computer 50 contains the license management device 520 which manages the license for exchanging various kinds of keys between the license administrative modules 511 in case the license from the distribution server 10 is received and the license by ripping is received between the distribution servers 10 or from the license administrative module 511, and reproducing the distributed encryption contents data in hard.

[0073] Drawing 7 is an outline block diagram for explaining the configuration of the playback terminal 102 shown in drawing 2.

[0074] The playback terminal 102 contains the controller 1106 for controlling actuation of the playback terminal 102 through the bus BS 3 and Bus BS 3 for performing data transfer of each part of the playback terminal 102, the control panel 1108 for giving the directions from the outside to the playback terminal 102, and the display panel 1110 for giving a user the information outputted from controller 1106 grade as vision information.

[0075] The removable memory card 110 for the playback terminal 102 to memorize the contents data (music data) from the distribution server 10 further, and perform decode processing, The memory card interface 1200 for controlling transfer of the data between a memory card 110 and a bus BS 3, In case encryption contents data and a license are received from a personal computer 50, the terminal 1114 for connecting the USB cable 70 with the USB interface 1112 for controlling the data transfer between a bus BS 3 and a terminal 1114 is included.

[0076] The playback terminal 102 contains the authentication data-hold section 1500 holding authentication data $\{KPp1//Cp1\}$ KPa enciphered in the condition that the justification can be further attested by decoding the class public presentation cryptographic key $KPp1$ and the class certificate $Cp1$ with the open authentication key KPa . Here, the class y of the playback terminal 102 presupposes that it is $y=1$.

[0077] The playback terminal 102 contains Kp1 attaching part 1502 which holds further Kp1 which is the decode key of a class proper, and the decode processing section 1504 which obtains the session key Ks2 which decoded the data which received from the bus BS 3 by Kp1, and was generated by the memory card 110.

[0078] The playback terminal 102 further The session key generating section 1508 which generates the session key Ks3 for enciphering the data which set and are carried out on a bus BS 3 between memory cards 110 in the playback session which reproduces the contents data memorized by the memory card 110 with a random number etc., In case the license key Kc and the playback control information ACp are received from a memory card 110 in the playback session of encryption contents data The session key Ks3 generated by the session key generating section 1508 is enciphered by the session key Ks2 obtained by the decode processing section 1504, and the encryption processing section 1506 outputted to a bus BS 3 is included.

[0079] Further, the playback terminal 102 decodes the data on a bus BS 3 by the session key Ks3, and contains the decode processing section 1510 which outputs the license key Kc and the playback control information ACp, and the decode processing section 1516 which decodes encryption contents data {Dc} Kc with the license key Kc decoded by the decode processing section 1510 in response to encryption contents data {Dc} Kc from the bus BS 3.

[0080] The playback terminal 102 contains the terminal 1530 for outputting further the output of the music playback section 1518 for reproducing contents data in response to the output from the decode processing section 1516, DA converter 1519 which changes the output of the music playback section 1518 into an analog signal from a digital signal, and DA converter 1519 to external output units (illustration abbreviation), such as a head telephone.

[0081] In addition, in drawing 7 , the field enclosed with a dotted line constitutes the contents regenerative circuit 1550 which decodes encryption contents data and reproduces music data.

[0082] On the other hand, the portable telephone 100 shown in drawing 1 has the function to receive distribution of encryption contents data or a license from the distribution server 10 through a cellular-phone network. Therefore, the function with which portable telephones, such as the transceiver section for changing into baseband signaling the configuration of the portable telephone 100 shown in drawing 1 in response to the signal from the antenna for receiving the signal by which a radio transmission is carried out with a cellular-phone network in the configuration shown in drawing 7 , and an antenna, or modulating the data from a portable telephone, and giving an antenna, a microphone, a loudspeaker, and a voice codec, are originally equipped is prepared.

[0083] About the actuation in each session of each component of a portable telephone 100 and the playback terminal 102, the back is explained to a detail using a flow chart.

[0084] Drawing 8 is an outline block diagram for explaining the configuration of a memory card 110 shown in drawing 1 and drawing 2 .

[0085] Although $KPmw$ and Kmw are prepared and the class certificate Cmw of a memory card is formed as the class public presentation cryptographic key of a memory card, and a class secret decode key as already explained, it shall be expressed with the natural number $w=3$ in a memory card 110. Moreover, the natural number x which identifies a memory card shall be expressed with $x=4$.

[0086] Therefore, a memory card 110 contains the authentication data-hold section 1400 holding authentication data $\{Kp3//Cm3\}$ KPa , the Kmc attaching part 1402 holding the individual secret decode key $Kmc4$ which is a decode key of the proper set up for every memory card, the Km attaching part 1421 holding the class secret decode key $Km3$, and the $KPmc$ attaching part 1416 holding the open cryptographic key $KPmc4$ which can be decoded with the individual secret decode key $Kmc4$.

[0087] Thus, by preparing the cryptographic key of a recording device called a memory card, it becomes possible to perform management of the distributed contents data or the enciphered license key per memory card so that it may become clear by the following explanation.

[0088] The interface 1424 with which a memory card 110 delivers further and receives a signal through a terminal 1426 between the memory card interfaces 1200, The bus BS 4 which exchanges a signal between interfaces 1424 The class secret decode key $Km3$ from the data given to a bus BS 4 from an interface 1424 is received from the Km attaching part 1421. The decode processing section 1422 which outputs the session key $Ks1$ which the distribution server 10 generated in the distribution session to Contact Pa , In response to the open authentication key KPa , the class certificate which performed decode processing with the open authentication key KPa from the data given to a bus BS 4 from the KPa attaching part 1414, and was obtained with a decode result for a controller 1420 With the decode processing section 1408 which outputs the obtained class public key to the encryption processing section 1410, and the key alternatively given by the change-over switch 1442 The encryption processing section 1406 which enciphers the data given alternatively and is outputted to a bus BS 4 with a change-over switch 1446 is included.

[0089] The session key generating section 1418 in which a memory card 110 generates the session key $Ks2$ in each session of distribution and playback further, The encryption processing section 1410 which enciphers the session key $Ks2$ which the session key generating section 1418 outputted by the class public presentation cryptographic keys $KPpy$ and $KPmw$ obtained by the decode processing section 1408, and is sent out to a bus BS 4, The decode processing section 1412 decoded by the session key $Ks2$ obtained from the session key generating section 1418 in response to the data enciphered by the session key $Ks2$ from the bus BS 4, The license key Kc and the playback control information ACp which were read from memory 1415 in the playback session of encryption contents data The cipher-processing section 1417 enciphered by the individual public presentation cryptographic key $KPmcx$ of

other memory cards 110 decoded in the decode processing section 1412 (!=4) is included.

[0090] The decode processing section 1404 for a memory card 110 to decode the data on a bus BS 4 further with the individual public presentation cryptographic key KPmc4 and the individual secret decode key Kmc4 of the memory card 110 which makes a pair, Encryption contents data {Dc} Kc and the license for reproducing encryption contents data {Dc} Kc (Kc, ACp, ACm, License ID, content ID), At the time of an effective flag, and the loan place ID and a loan, License ID and additional information Dc-inf, The memory 1415 for storing in response to the playback list file which manages the encryption contents data stored in a memory card 110, and the license management file for managing a license from a bus BS 4 is included. Memory 1415 is constituted by semiconductor memory. Moreover, memory 1415 consists of license field 1415A and data area 1415B. License field 1415A is a field for recording License ID at the time of the license, effective flag, and loan place ID and a loan. Data area 1415B is a field for recording the playback list file which records the fundamental information for accessing the license management file which records information required in order to manage related information Dc-inf of the encryption contents data {Dc} Kc and encryption contents data, and a license for every encryption contents, and encryption contents data and the license which were recorded on the memory card. And the exterior to direct access is possible for data area 1415B. About the detail of a license management file and a playback list file, it mentions later.

[0091] License field 1415A stores License ID per record only for licenses called an entry at the time of the license, effective flag, and loan place ID and a loan, in order to record License ID at the time of the license (license key Kc, playback control information ACp, access-restriction information ACm, License ID, content ID), effective flag, and loan place ID and a loan. In accessing to a license etc., the license etc. has the composition of it being stored or specifying an entry recording a license etc. by the entry number.

[0092] Further, a memory card 110 performs data transfer between the exteriors through a bus BS 4, and contains the controller 1420 for controlling actuation of a memory card 110 in response to playback information etc. between buses BS 4.

[0093] In addition, license field 1415A is constituted by the Tampa-proof module field. Moreover, license field 1415A and data area 1415B do not need to be constituted in one memory 1415, and may be constituted separately, respectively. Furthermore, memory 1415 may be a field only for licenses without data area 1415B.

[0094] Drawing 9 is the outline block diagram showing the configuration of the license management device 520 built in the personal computer 50. It is only that points equipped with the interface 5224 with which the function of the point which does not need the field equivalent to data area 1415B in MEMOKADO 110, and an interface 1424 differs from the configuration of a terminal 1426, and a terminal 5226 differ, and the license management device 520 consists of the same configuration as a memory card 110 fundamentally. The

authentication data-hold section 5200 of the license management device 520, the Kmc attaching part 5202, the decode processing section 5204, the cipher-processing section 5206, the decode processing section 5208, the cipher-processing section 5210, the decode processing section 5212, the KPa attaching part 5214, the KPmc attaching part 5216, The cipher-processing section 5217, the session key generating section 5218, a controller 5220, the Km attaching part 5221, the decode processing section 5222, an interface 5224, a terminal 5226, and change-over switches 5242 and 5246 Respectively The authentication data-hold section 1400 of a memory card 110, the Kmc attaching part 1402, the decode processing section 1404, the cipher-processing section 1406, the decode processing section 1408, the cipher-processing section 1410, the decode processing section 1412, the KPa attaching part 1414, the KPmc attaching part 1416, the cipher-processing section 1417, It is the same as the session key generating section 1418, a controller 1420, the Km attaching part 1421, the decode processing section 1422, and change-over switches 1442 and 1446. However, the authentication data-hold section 5200 holds authentication data {K_{Pm7}//C_{m7}} KPa, the KPmc attaching part 5216 holds the individual public presentation cryptographic key K_{Pm8}, the Km attaching part 5202 holds the class secret decode key K_{m7}, and the Kmc attaching part 5221 holds the individual secret decode key K_{mc8}. The natural number w showing the class of the license management device 520 is w= 7, and the natural number x for identifying the license management device 520 presupposes that it is x= 8.

[0095] The license management device 520 replaces with and contains in the memory 1415 of a memory card 110 a license (K_c, AC_p, AC_m, License ID, content ID), an effective flag, and the memory 5215 that records License ID at the time of the loan place ID and a loan. Memory 5215 contains license field 5215A which recorded License ID at the time of the license, effective flag, and loan place ID and a loan.

[0096] Hereafter, actuation of each session in the data distribution system shown in drawing 1 and drawing 2 is explained.

[0097] [Distribution] drawing 10 and drawing 11 are the 1st and 2nd flow charts for explaining the distribution session which occurs at the time of the purchase of the encryption contents data in the personal computer 50 of the data distribution system shown in drawing 1 and drawing 2 , and a license. In addition, this actuation is called "distribution."

[0098] Before the processing in drawing 10 , the user of a personal computer 50 connects through the Internet network 30 to the distribution server 10, and is premised on acquiring the content ID to the contents which wish to purchase.

[0099] With reference to drawing 10 , the distribution request by assignment of content ID is made through a keyboard 560 from the user of a personal computer 50 (step S100). And the purchase conditions AC for purchasing the license of encryption contents data through a keyboard 560 are inputted (step S102). That is, in order to purchase the license key K_c which decodes selected encryption contents data, the purchase conditions AC are inputted

supposing the access control information ACm and the playback control information ACp of encryption contents data.

[0100] If the purchase conditions AC of encryption contents data are inputted, a controller 510 will give output directions of authentication data to the license management device 520 through a bus BS 2 (step S104). The controller 5220 of the license management device 520 receives the Request to Send of authentication data through a terminal 5226, an interface 5224, and a bus BS 5 (step S106). And through a bus BS 5, read-out is minded for authentication data {K_{Pm7}//C_{m7}} K_{Pa} from the authentication data hold section 5200, it minds a bus BS 5, an interface 5224, and a terminal 5226 for {K_{Pm7}//C_{m7}} K_{Pa}, and a controller 5220 outputs (step S108).

[0101] In addition to authentication data {K_{Pm3}//C_{m3}} K_{Pa} from the license management device 520, the controller 510 of a personal computer 50 transmits Data AC and the distribution request of content ID and license purchase conditions to the distribution server 10 through a modem 555 and the Internet network 30 (step S110).

[0102] In the distribution server 10, the data AC of a distribution request, content ID, authentication data {K_{Pm7}//C_{m7}} K_{Pa}, and license purchase conditions are received from a personal computer 50 (step S112), and decode processing is performed for the authentication data outputted from the license management device 520 in the decode processing section 312 with the open authentication key K_{Pa} (step S114).

[0103] Authentication processing which judges whether the distribution control section 315 received the authentication data enciphered from the decode processing result in the decode processing section 312 for proving the justification in the engine of normal is performed (step S116). When it is judged that it is just authentication data, the distribution control section 315 recognizes and receives the class public presentation cryptographic key K_{Pm7} and the class certificate C_{m7}. And it shifts to the next processing (step S118). In not being just authentication data, it supposes un-recognizing, and it ends a distribution session without receiving the class public presentation cryptographic key K_{Pm7} and the class certificate C_{m7} (step S166).

[0104] If it is checked that it is access from the personal computer which equipped with the license management device with just authentication data as a result of authentication, in the distribution server 10, the session key generating section 316 will generate the session key K_{s1} for distribution (step S118). The session key K_{s1} is enciphered by the encryption processing section 318 by the class public presentation cryptographic key K_{Pm7} corresponding to the memory card 110 obtained by the decode processing section 312 (step S120).

[0105] The distribution control section 315 generates License ID (step S122), and License ID and the enciphered session key K_{s1} are outputted outside through a bus BS 1 and a communication device 350 as license ID//{K_{s1}} K_{m3} (step S124).

[0106] If a personal computer 50 receives license ID//{Ks1} Km7, a controller 510 will input license ID//{Ks1} Km7 into a memory card 110 (step S126). If it does so, in the license management device 520, a controller 5220 will receive license ID//{Ks1} Km7 through a terminal 5226 and an interface 5224 (step S128). And when {Ks1} Km7 is given to the decode processing section 5222 through a bus BS 5 and the decode processing section 5222 carries out decode processing with the class secret decode key Km3 peculiar to the license management device 520 held at the Km attaching part 5221, a controller 5220 decodes the session key Ks1, and receives the session key Ks1 (step S130).

[0107] A controller 5220 directs generation of the session key Ks2 generated in the license management device 520 to the session key generating section 5218 at the time of distribution actuation, if acceptance of the session key Ks1 generated by the distribution server 10 is checked. And the session key generating section 5218 generates the session key Ks2 (step S132).

[0108] By the session key Ks1 given from the decode processing section 5222 through the contact Pa of a change-over switch 5242, the encryption processing section 5206 enciphers the session key Ks2 given by switching the contact of a change-over switch 5246 one by one, and the individual public presentation cryptographic key KPmc8 as one data stream, and outputs {Ks2//KPmc8} Ks1 to a bus BS 5. Encryption {data KPmc 8} Ks2// Ks1 outputted to the bus BS 5 are outputted to a personal computer 50 through an interface 5224 and a terminal 5226 from a bus BS 5 (step S134), and is transmitted to the distribution server 10 from a personal computer 50 (step S136).

[0109] With reference to drawing 11, the distribution server 10 receives {Ks2//KPmc4} Ks1, decode processing by the session key Ks1 is performed in the decode processing section 320, and the open cryptographic key KPmc8 of a proper is received to the session key Ks2 generated with the license management device 520, and the license management device 520 (step S138).

[0110] The distribution control section 315 determines the access-control information ACm and the playback control information ACp according to the data AC of the license purchase conditions which acquired the license key Kc from the information database 304 according to the content ID acquired at step S112 (step S140), and were acquired at step S112 (step S142).

[0111] The distribution control section 315 gives the generated license ID, i.e., a license, content ID, the license key Kc, the playback control information ACp, and the access-control information ACm to the encryption processing section 326. To the license management device 520 obtained by the decode processing section 320, by the open cryptographic key KPmc8 of a proper, the encryption processing section 326 enciphers a license and generates encryption data {license ID// content ID//Kc//ACm//ACp} Kmc8 (step S144). And the encryption processing section 328 enciphers encryption data {license ID// content ID//Kc//ACm//ACp} Kmc8 from the encryption processing section 326 by the session key Ks2 from the decode

processing section 320, and outputs encryption data {{license ID// content ID//Kc//ACm//ACp} Kmc8} Ks2. The distribution control section 315 transmits encryption data {{license ID// content ID//Kc//ACm//ACp} Kmc8} Ks2 to a personal computer 50 through a bus BS 1 and a communication device 350 (step S146).

[0112] A personal computer 50 receives transmitted encryption data {{license ID// content ID//Kc//ACm//ACp} Kmc8} Ks2, and inputs it into the license management device 520 through a bus BS 2 (step S148). In the license management device 520, the received data given to the bus BS 5 are decoded by the decode processing section 5212 through a terminal 5226 and an interface 5224. The decode processing section 5212 decodes the received data of a bus BS 5 using the session key Ks2 given from the session key generating section 5218, and outputs them to a bus BS 5 (step S150).

[0113] this -- a phase -- a bus -- BS -- five -- **** -- Kmc -- an attaching part -- 5202 -- holding -- having -- secret -- decode -- a key -- Kmc -- eight -- decode -- being possible -- encryption -- a license -- {-- a license -- ID -- /-- /-- content ID -- /-- /-- Kc -- /-- /-- ACm -- /-- /-- ACp --} -- Kmc -- eight --} -- outputting -- having (step S150) .

[0114] Encryption license {license ID// content ID//Kc//ACm//ACp} Kmc8 is decoded with the individual secret decode key Kmc8 in the decode processing section 5204 by directions of a controller 5220, and a license (the license key Kc, License ID, content ID, the access-control information ACm, and playback control information ACp) is received by them (step S152).

[0115] The controller 510 of a personal computer 50 determines the entry number for storing the license received from the distribution server 10 based on the license management file read from HDD530, and inputs the determined entry number into the license management device 520 through a bus BS 2. And a controller 510 carries out renewal of an addition of the license management information of a license management file (step S154).

[0116] If it does so, it will judge whether the controller 5220 of the license management device 520 can lend out the acquired license based on the access-control information ACm acquired in step S152 (step S156). The access-control information ACm consists of duplicate / migration control information and the count control information of playback. Either "1", "2" and "3" are set up as duplicate / migration control information, "1" means duplicate / migration failure of a license, "2" means duplicate improper - migration C, and "3" means prohibition of a duplicate and migration. Moreover, the value of 0-255 is set up as count control information of playback. And the value of 0-254 means that playback of encryption contents data is possible only for the count of the set-up value, and 255 means that encryption contents data are reproducible without any restriction. In this invention, when duplicate / migration control information is set as "2" and the count control information of playback is set as "255", a license shall be lent out. In addition, it is an indispensable condition for enabling the loan of a license that the count control information of playback is set as "255." Since it is difficult to manage how many times encryption contents data were

reproduced at the loan place the lending out agency by the count of playback having a limit when the count control information of playback is set as "0-254", when the count of playback is finite, the loan of a license is forbidden, when the count of playback is infinity, it restricts, and the loan of a license is made possible.

[0117] And if the loan of a license is possible for a controller 5220, the loan flag stored in the field specified by the entry number of license field 5215A of memory 5215 will be set as "good" (step S158). On the other hand, in step S156, when judged with the loan of a license being impossible, a controller 5220 sets as "improper" the loan flag stored in the field specified by the entry number of license field 5215A (step S160).

[0118] A controller 5220 after step S158 or step S160 The effective flag stored in the field specified by the entry number of license field 5215A is set as "effective" (step S162). The license (License ID, content ID, the license key Kc, the access-control information ACm, and playback control information ACp) received in step S152 to the field specified by the entry number of license field 5215A is stored (step S164). And distribution actuation of a license is ended (step S166).

[0119] After distribution actuation of a license is completed, the controller 510 of a personal computer 50 transmits the distribution demand of encryption contents data to the distribution server 10, and the distribution server 10 receives the distribution demand of encryption contents data. And from the information database 304, the distribution control section 315 of the distribution server 10 acquires encryption contents data {Dc} Kc and additional information Dc-inf, and outputs these data through a bus BS 1 and a communication device 350.

[0120] A personal computer 50 receives {Dc} Kc/Dc-inf, and receives encryption contents data {Dc} Kc and additional information Dc-inf. If it does so, a controller 1106 will input encryption contents data {Dc} Kc and additional information Dc-inf into HDD530 through a bus BS 2 as one contents file. Moreover, a controller 510 generates the license management file to encryption contents data {Dc} Kc and additional information Dc-inf containing the entry number of the license stored in the license management device 520, and License ID and content ID of a plaintext, and inputs it into HDD530 through a bus BS 2. Furthermore, a controller 510 adds the name of the recorded contents file and a license management file, the information (a music name, artist name) about the encryption contents data extracted from additional information Dc-inf, etc. as information on the contents received to the contents list file currently recorded on HDD530, and the whole processing ends it.

[0121] Thus, after checking that the open cryptographic key KPm7 which has enciphered and transmitted to that the license management device 520 built in the personal computer 50 is a device holding the authentication data of normal and coincidence with the class certificate Cm7 is effective, a license can be distributed, and distribution of the license to an inaccurate license management device can be forbidden.

[0122] Furthermore, by exchanging the cryptographic key generated with a distribution server and the license ***** device 520, respectively, performing encryption using the cryptographic key which each received, and transmitting the encryption data to the other party, de facto mutual recognition can be performed also in transmission and reception of each encryption data, and the security of a data distribution system can be raised.

[0123] Actuation which distributes a license is also directly performed according to the flow chart shown in drawing 10 and drawing 11 to the memory card 110 with which the portable telephone 100 was equipped in the data distribution system shown in drawing 1 . Namely, what is necessary is to replace a personal computer 50 with a portable telephone 100, and just to replace the license management device 520 with a memory card 110 in the above-mentioned explanation. Moreover, in step S108 of drawing 10 , authentication data {K_{Pm3}//C_{m3}} K_{Pa} is outputted from a memory card 110 instead of authentication data {K_{Pm7}//C_{m7}} K_{Pa}. Others are the same as having mentioned above.

[0124] The user of [ripping] personal computer 50 can acquire and use music data from the music CD which encryption contents data and a license are acquired by distribution, and also is owned. Although digital reproduction of Music CD may not be freely performed from the position of right protection of a copyright person, he is allowed for an individual to reproduce using a tool equipped with a copyright protection feature for the self purpose of use, and to enjoy music. Then, the license administrative module 511 acquires music data from Music CD, and also includes the program which realizes the ripping function which generates encryption contents data manageable [with the license administrative module 511] and a license.

[0125] Moreover, there are some which inserted digital watermarking called a water mark in music data in the music CD in recent years. The range of the use in a user is written in this water mark by the copyright person as a use regulation. It is necessary to surely follow this use regulation from the point of protection of copyrights in ripping from the music data with which the use regulation is written in. Henceforth, suppose that the code of duplicate conditions (the generation and duplicate which can be reproduced [duplicate prohibition /] are possible), the shelf-life of a duplicate, the number of the maximum check-out, edit, reproduction speed, and a refreshable area, the count limit of playback to a duplicate, and available time are indicated as a use regulation. Moreover, when a water mark is not detected, there is the conventional music CD in which the use regulation is not written.

[0126] Moreover, ripping may digitize the music signal which music data were acquired directly and also was inputted as an analog signal, and may acquire it from Music CD as music data. Furthermore, in order to reduce the amount of data, it is also possible to consider the music data by which compression coding was carried out as an input. Furthermore, it is also possible to incorporate as an input the contents data distributed by distribution systems other than the distribution system by the gestalt of this operation.

[0127] With reference to drawing 12 and drawing 13 , acquisition of the encryption contents data based on ripping from the music CD on which music data were recorded, and a license is explained.

[0128] Drawing 12 is the functional block diagram showing the function of the software which carries out ripping of the music data which CD-ROM drive 540 contained in the personal computer 50 shown in drawing 6 read from CD. The software which carries out ripping of the music data is equipped with the water mark detection means 5400, the water mark judging means 5401, the remark means 5402, the license generating means 5403, the music encoder 5404, and the cryptographer stage 5405.

[0129] The water mark detection means 5400 detects a water mark, and extracts the use regulation indicated from the music data acquired from Music CD. The water mark judging means 5401 judges the propriety of ripping based on the use regulation indicated by the water mark, when it is able to be detected further whether it was detectable, the detection result, i.e., the water mark, of the water mark detection means 5400. In this case, what the use regulation to which does not have the use regulation of a water mark or the duplicate and the migration of music data recorded on Music CD were permitted was recorded by the water mark for when ripping is good means, and when ripping is improper, what the use regulation which must not reproduce and move the music data recorded on Music CD was recorded by the water mark for means.

[0130] Ripping is possible for the judgment result in the water mark judging means 5401, and the remark means 5402 changes the water mark included in music data for the water mark which changed the duplicate conditions of music data, when there are directions of a duplicate generation (i.e., when music data may be reproduced and moved). However, when considering as an input the music data encoded when ripping of the analog signal was inputted and carried out, and in considering the music data distributed by other distribution systems as an input, if ripping is possible, it will not be concerned with the contents of the use regulation, but will surely change a water mark. In this case, when there are directions of a duplicate generation, the contents of the use regulation are changed, and when other, the acquired use regulation is used as it is.

[0131] The license generating means 5403 generates a license based on the judgment result of the water mark judging means 5401. The music encoder 5404 encodes the music data to which the remark of the water mark was carried out by the remark means 5402 to a predetermined method. The cryptographer stage 5405 enciphers the music data from the music encoder 5404 with the license key Kc contained in the license generated by the license generating means 5403.

[0132] With reference to drawing 13 , the ripping actuation in the controller 510 of a personal computer 50 is explained. If ripping actuation is started, the water mark detection means 5400 will detect the use regulation of a water mark based on the data detected from Music

CD (step S800). And it judges whether the water mark judging means 5401 can be reproduced based on the use regulation currently recorded as the detection result and water mark of the water mark detection means 5400 (step S802). A water mark is detected, and when a duplicate is permitted under a use regulation and the contents of the use regulation can respond in the access-control information and playback control information within a license, it is judged that ripping is good and it shifts to step S804. Moreover, when a water mark is detected and the use regulation [that it cannot respond in the access-control information or playback control information within prohibition of a duplicate or a license] is indicated by the use regulation, it is judged as prohibition of ripping, it shifts to step S828, and ripping actuation is ended. When the water mark is not included in CD with which it was equipped, it shifts to step S810.

[0133] In step S802, when it is judged that ripping is good, music data are incorporated from Music CD and the water mark included in music data by the remark means 5402 is changed for the water mark which changed duplicate conditions (step S806). That is, a duplicate generation is changed for the water mark made into 2 times when the use regulation of a water mark has permitted the duplicate to three generations. And the license generating means 5403 generates the license reflecting a use regulation. That is, the license generating means 5403 generates the license whose count of a duplicate is two generations (step S806).

[0134] On the other hand, in step S802, when a water mark is not detected, migration / duplicate control information which the license generating means 5403 forbade only the duplicate of a license generates the license of "2" (step S810).

[0135] After steps S806 or S810, the music encoder 5404 encodes the music data with which the remark of the water mark was carried out to a predetermined method, and generates the contents data Dc (step S814). And the cryptographer stage 5405 enciphers with the license key Kc contained in the license generated by the license generating means 5403 in the music data from the music encoder 5404, and generates encryption contents data {Dc} Kc (step S816). Then, additional information Dc-inf of contents data {Dc} is generated by the user input inputted from the keyboard 560 of the information included in Music CD, or a personal computer 50 (step S818).

[0136] If it does so, the controller 510 of a personal computer 50 will acquire encryption contents data {Dc} Kc and additional information Dc-inf through a bus BS 2, and will record them on HDD530 (step S820). And a controller 510 stores the generated license (Transaction ID, content ID, the license key Kc, the access-restriction information ACm, playback control information ACp) in the license management device 520 (step S822). According to step S166, it is carried out from step S104 of the flow chart shown in drawing 10 and drawing 11 through the license administrative module 511 to the license management device 520 with which storing of a license is performed on the controller 510. That is, the license administrative module 511 working on a controller 510 is the program which can realize the

function corresponding to distribution of the license in the distribution server 10 that what is necessary is just to replace the distribution server 10 with a controller 510 in encryption contents data and the explanation in distribution of a license. Then, a controller 510 generates the license management file to encryption contents data {Dc} Kc and additional information Dc-inf which were recorded on HDD, including Transaction ID and content ID of a plaintext, and records it on HDD530 (step S824). Finally, a controller 510 adds the file name of the contents received to the contents list file currently recorded on HDD530 (step S826), and ripping actuation ends it (step S828).

[0137] Thus, the license which could acquire encryption contents data and a license and was acquired from Music CD by ripping is protected and managed with the contents distributed from the distribution server 10.

[0138] Thus, the encryption contents data and the license which were acquired from Music CD by ripping are generated by the license administrative module 511, and are managed like the encryption contents data and the license which were received from the distribution server 10. Therefore, a personal computer 50 is ready-for-sending ability in the memory card 110 with which the portable telephone 100 or the playback terminal 102 was equipped by the check-out which mentions later the encryption contents data and the license which were acquired from Music CD by ripping. By this, the user of a portable telephone 100 or the playback terminal 102 can receive the encryption contents data which the personal computer 50 acquired by ripping to the self memory card 110, and can enjoy playback.

[0139] In the above, although the personal computer 50 acquired encryption contents data and a license from Music CD by ripping, it may generate encryption contents data and a license by ripping in this invention from the contents data received not only by this but by other Internet distribution.

[0140] As [migration] **** was carried out, a memory card 110 and the license management device 520 can acquire encryption contents data and a license from the distribution server 10. Then, actuation in case a memory card 110 or the license management device 520 moves the license received from the distribution server 10 to other memory cards is explained.

[0141] Drawing 14 and drawing 15 are the 1st and 2nd flow charts for explaining the actuation for which the license management device 520 moves the encryption contents data and the license which were received from the distribution server 10 to the memory card 110 equipped by the portable telephone 100 or the playback terminal 102 in the data distribution system shown in drawing 1 and drawing 2 . In migration, since a portable telephone 100 or the playback terminal 102 is the device of only relaying data, it has been omitted from the flow chart. In explaining migration, the case where it moves to the memory card 110 with which the portable telephone 100 of drawing 1 was equipped is explained, but the same is said of the case where it moves to the memory card 110 with which the playback terminal 102 of drawing 2 was equipped, and reading ***** is good for the playback terminal 102 in a

portable telephone 100. Moreover, when moving to the license management device 520 from a memory card 110, reading ***** is good in the license management device 520 and a memory card 110 similarly.

[0142] In addition, before the processing in drawing 14 , according to a contents list file, the user of a personal computer 50 determines the contents which move, and explains as a premise that the contents file and the license management file can be specified. Moreover, the controller 510 is premised on holding the license management file.

[0143] If a migration request is inputted from the keyboard 560 of a personal computer 50 with reference to drawing 14 (step S300), a controller 510 will transmit the Request to Send of authentication data to a memory card 110 through the USB interface 550, a terminal 580, and the USB cable 70 (step S302). And the controller 1420 of a memory card 110 receives the Request to Send of authentication data through a terminal 1426, an interface 1424, and a bus BS 4 (step S304).

[0144] A controller 1420 will output read-out and its read authentication data {K_{Pm3}//C_{m3}} K_{Pa} for authentication data {K_{Pm3}//C_{m3}} K_{Pa} to the exterior through a bus BS 4, an interface 1424, and a terminal 1426 through a bus BS 4 from the authentication data-hold section 1400, if the Request to Send of authentication data is received (step S306). And the controller 510 of a personal computer 50 transmits authentication data {K_{Pm3}//C_{m3}} K_{Pa} for authentication data {K_{Pm3}//C_{m3}} K_{Pa} to the license management device 520 through a receipt and a bus BS 2 through a terminal 580 and the USB interface 550 (step S308).

[0145] If it does so, the controller 5220 of the license management device 520 will receive authentication data {K_{Pm3}//C_{m3}} K_{Pa} through a terminal 5226 and an interface 5224, and will give the authentication data {K_{Pm3}//C_{m3}} K_{Pa} which received to the decode processing section 5208 through a bus BS 5. And the decode processing section 5208 performs decode processing of authentication data {K_{Pm3}//C_{m3}} K_{Pa} with the authentication key K_{Pa} from the K_{Pa} attaching part 5214 (step S310). A controller 5220 performs authentication processing which judges whether the authentication data which gave the code for proving the justification in the engine of normal were received, in order to attest that whether processing having been performed normally and a memory card 110 hold the class public presentation cryptographic key K_{Pm3} and the class certificate C_{m3} from a memory card of normal from the decode processing result in the decode processing section 5208 (step S312). When it is judged that it is just authentication data, a controller 5220 recognizes and receives the class public presentation cryptographic key K_{Pm3} and the class certificate C_{m3}. And it shifts to the next processing (step S314). In not being just authentication data, it supposes un-recognizing, and it ends processing without receiving the class public presentation cryptographic key K_{Pm3} and the class certificate C_{m3} (step S374).

[0146] If it is checked as a result of authentication that it is a memory card with just authentication data, in the license management device 520, a controller 5220 will control the

session key generating section 5218, and the session key generating section 5218 will generate session key Ks2a for migration (step S314). Session key Ks2a is enciphered by the encryption processing section 5210 by the class public presentation cryptographic key KPm3 corresponding to the memory card 110 obtained by the decode processing section 5208. And a controller 5220 acquires encryption {Ks2data a} Km3 through a bus BS 5, and outputs encryption {Ks2data a} Km3 through a bus BS 5, an interface 5224, and a terminal 5226 (step S316).

[0147] A controller 510 receives {Ks2a} Km3 from the license management device 520 through a bus BS 2 (step S318), and acquires License ID from the license management information currently recorded on HDD530 (step S320). And a controller 510 is transmitted to the memory card 110 which the acquired license ID and encryption {Ks2data a} Km3 received in step S318 were used as one data, and was equipped with license ID//{Ks2a} Km3 by the portable telephone 100 through the terminal 580 and the USB interface 550 (step S322). If it does so, the controller 1106 of a memory card 110 will receive license ID//{Ks2a} Km3 through a terminal 1426, an interface 1424, and a bus BS 4 (step S324). Then, a controller 1420 gives encryption {Ks2data a} Km3 to the decode processing section 1422, and with the class secret decode key Km3 from the Km attaching part 1421, the decode processing section 1422 decodes {Ks2a} Km3, and receives session key Ks2a (step S326). And the session key generating section 1418 generates session key Ks2b (step S328), and the encryption processing section 1406 enciphers session key Ks2b acquired by switching the terminal of a change-over switch 1446 one by one, and the individual public presentation cryptographic key KPmc4 by session key Ks2a decoded by the decode processing section 1404, and it generates Ks2b//encryption {data KPmc 4} Ks2a. A controller 1420 outputs Ks2b//encryption {data KPmc 4} Ks2a through a bus BS 4, an interface 1424, and a terminal 1426 (step S330), and the controller 510 of a personal computer 50 receives Ks2b//encryption {data KPmc 4} Ks2a through a terminal 580 and the USB interface 550. And a controller 510 transmits Ks2b//encryption {data KPmc 4} Ks2a to the license management device 520 through a bus BS 2 (step S332).

[0148] If it does so, the controller 5220 of the license management device 520 will receive Ks2b//encryption {data KPmc 4} Ks2a through a terminal 5226, an interface 5224, and a bus BS 5, and will give its Ks2b// encryption {data KPmc 4} Ks2a which received to the decode processing section 5212. By session key Ks2a from the session key generating section 5218, the decode processing section 5212 decodes Ks2b//encryption {data KPmc 4} Ks2a, and receives session key Ks2b and the open cryptographic key KPmc4 (step S334).

[0149] Then, a controller 510 acquires the entry number in which the license set from the license management information corresponding to the license management device 520 as the object of migration is stored (step S336), and inputs the acquired entry number and a migration demand of a license into the license management device 520 (step S338). The

controller 5220 of the license management device 520 receives an entry number and a migration demand of a license through a terminal 5226, an interface 5224, and a bus BS 5, and acquires a license (License ID, content ID, the license key Kc, the access-control information ACm, playback control information ACp) from the entry of license field 5215A of the memory 5215 specified by the received entry number (step S340).

[0150] With reference to drawing 15, a controller 5220 judges the existence of a loan of the license acquired in step S340 with a loan flag (step S342). And migration actuation will be ended if the acquired license is lending out (step S374). If the acquired license is not lending [be / it] out, subsequently as for a controller 5220, the access-control information ACm will be checked (step S344). That is, a controller 5220 checks whether based on the acquired access-control information ACm, the license which is going to move to a memory card 110 is the license which cannot perform playback of encryption contents data by the count of playback first. It is because there is no semantics which cannot reproduce encryption contents data according to a license, but moves the encryption contents data and license to a memory card 110 when the count of playback does not remain (the count of playback = 0). When it cannot reproduce and can reproduce, the duplicate of a license and the propriety of migration are judged by migration / duplicate control information.

[0151] In step S344, the count of playback of encryption contents data is not made (the count of playback = 0), or when migration / duplicate flag is the ban (= 0) on a migration duplicate, using the access-control information ACm, it judges that duplicate migration is impossible, and shifts to step S374, and migration actuation is ended. In step S344, playback of encryption contents data can be performed (count != of playback 0), and migration / duplicate control information is judged to be migration of a license in the case of C "=2", and only migration carries out the invalid of the effective flag in the entry number as which the controller 5220 was specified in license field 5215A of memory 5215 (step S346). Moreover, playback of encryption contents data can be performed, it is judged that it is the duplicate of a license when "count != of playback 0" and a duplicate of migration / duplicate control information are good, and it shifts to step S348, without performing step S346.

[0152] After step S344 or step S346, the encryption processing section 5217 enciphers a license to the memory card 110 obtained by the decode processing section 5212, and generates encryption data {license ID// content ID//Kc//ACm//ACp} Kmc4 by the open cryptographic key KPmc4 of a proper to it (step S348). Thus, when the duplicate of a license is permitted, in order to make a license usable in both duplicate places a reproducing agency, it is made to process step S348, after making the effective flag of license field 5215A into an invalid (step S346 reference), when migration of a license is possible, but to shift to step S348, without minding step S346 which makes the effective flag of a license an invalid. Therefore, when moving a license, a license cannot be read from the license management device 520.

[0153] The encryption processing section 5206 minds the contact Pc of a switch 5246 for

encryption data {license ID// content ID//Kc//ACm//ACp} Kmc4 enciphered by the encryption processing section 5217. And a receipt, A receipt and encryption data {license ID// content ID//Kc//ACm//ACp} Kmc4 are enciphered for session key Ks2b decoded by the decode processing section 5212 with session key Ks2b through the contact Pb of a switch 5242. And a controller 5220 outputs encryption data {{license ID// content ID//Kc//ACm//ACp} Kmc4} Ks2b through a bus BS 5, an interface 5224, and a terminal 5226 (step S350).

[0154] A controller 510 receives encryption data {{license ID// content ID//Kc//ACm//ACp} Kmc4} Ks2b from a memory card 120 through a bus BS 2, and transmits the received encryption data {{license ID// content ID//Kc//ACm//ACp} Kmc4} Ks2b to a memory card 110 (step S352).

[0155] The controller 1420 of a memory card 110 gives encryption data {{license ID// content ID//Kc//ACm//ACp} Kmc4} Ks2b to the decode processing section 1412 in response to the input of encryption data {{license ID// content ID//Kc//ACm//ACp} Kmc4} Ks2b through a terminal 1426, an interface 1424, and a bus BS 4. And the decode processing section 1412 decodes encryption data {{license ID// content ID//Kc//ACm//ACp} Kmc4} Ks2b with session key Ks2b generated by the receipt and the session key generating section 1418 through the bus BS 4, and receives {license ID// content ID//Kc//ACm//ACp} Kmc4 (step S354).

[0156] Then, encryption data {license ID// content ID//Kc//ACm//ACp} Kmc4 is decoded by directions of a controller 1420 with the secret decode key Kmc4 in the decode processing section 1404, and a license (the license key Kc, License ID, content ID, the access-control information ACm, and playback control information ACp) is received by them (step S356).

[0157] If it does so, while a controller 510 will determine the entry number for storing the license moved / reproduced from the license management information of the memory card 110 which is a receiving side and will input it into a memory card 110, the license management information of a receiving side (memory card 110) is updated (step S358).

[0158] If it does so, it will judge whether the controller 1420 of a memory card 100 can lend out the acquired license based on the access-control information ACm acquired in step S356 (step S360). And if the loan of a license is possible for a controller 1420, the loan flag stored in the field specified by the entry number of license field 1415A of memory 1415 will be set as "good" (step S362). On the other hand, in step S360, when judged with the loan of a license being impossible, a controller 1420 sets as "improper" the loan flag stored in the field specified by the entry number of license field 1415A (step S364).

[0159] A controller 1420 after step S362 or step S364 The effective flag stored in the field specified by the entry number of license field 1415A is set as "effective" (step S366). The license (License ID, content ID, the license key Kc, the access-control information ACm, and playback control information ACp) received in step S356 to the field specified by the entry number of license field 1415A is stored (step S368).

[0160] On the other hand, it judges whether migration or the duplicate of a license is possible

for a controller 510 after step S358 (step S370), and when movable, the license management information of a transmitting side, i.e., the license management information currently recorded on HDD530 corresponding to the license which moved, is deleted, and the license management file currently recorded on data area 1415B of the license management information of a transmitting side and a memory card 110 is rewritten (step S372). In step S370, when judged with the loan of a license being possible, migration actuation of a license is ended after step S372 or step S368 (step S374).

[0161] In addition, what is necessary is just to perform migration to the memory card 110 of encryption contents data from a memory card 120 by reading encryption contents data from data area 1415B of a memory card 120, and transmitting to a memory card 110, after migration of a license is completed.

[0162] Thus, after checking that the open cryptographic key KPm3 which has enciphered and transmitted to that the memory card 110 with which the portable telephone 100 was equipped is the device of normal, and coincidence with the class certificate Cm3 is effective, a license can be moved only to the migration demand to a regular memory card, and migration to an inaccurate memory card can be forbidden.

[0163] Moreover, by exchanging the cryptographic key generated by the memory card, performing encryption using the cryptographic key which each received, and transmitting the encryption data to the other party, de facto mutual recognition can be performed also in transmission and reception of each encryption data, and the security in actuation of migration of a license can be raised.

[0164] Moreover, migration of a license is also performed according to the flow chart from the memory card 110 to the license management device 520 shown in drawing 14 and drawing 15 . That is, in drawing 1 , a portable telephone 100 will receive distribution and the encryption contents data and the license which were stored in the memory card 110 can be evacuated to a personal computer 50.

[0165] Moreover, that a personal computer 50 can move the license received from the distribution server 10 to a memory card 110 is only the license which the license management device 520 received in hard from the distribution server 10, and the license by which ripping was carried out with the license administrative module 511 from Music CD is unmovable. Then, ripping is carried out with the license administrative module 511, and it enabled it to transmit the license recorded on the license management device 520 to a memory card 110 by the concept of the check-out (loan) explained below and check-in (return).

[0166] Moreover, the loan of the license to a memory card 110 from a memory card 120 and return are also possible. The difference with "migration" and "a loan" "migration" In the memory card of the transmitting origin to which the license was moved Since the effective flag of a license is set as the invalid (step S346 reference of drawing 15), "migration" Although encryption contents data and a license cannot be acquired from the memory card of

a transmitting agency and encryption contents data cannot be reproduced, "a loan" It is in the point which can acquire encryption contents data and a license from the memory card of the loan origin which lent out the license, and can reproduce encryption contents data. Moreover, as mentioned above, the license which carried out ripping from Music CD is sent.

[0167] In the data distribution system shown in [loan] drawing 1 and drawing 2 , the actuation transmitted in order to lend out the encryption contents data and the license by which were distributed to the license management device 520 from the distribution server 10, or ripping was carried out from Music CD to a memory card 110 on the assumption that return is explained. In addition, this actuation is called "loan."

[0168] Drawing 16 and drawing 17 are the 1st and 2nd flow charts for [from the license management device 520 to a memory card 110] explaining the loan of a license.

[0169] In addition, before the processing in drawing 16 , according to a contents list file, the user of a portable telephone 100 determines the contents which move, and explains as a premise that the contents file and the license management file can be specified. Moreover, the controller 40 is premised on holding the license management file.

[0170] If a loan request is inputted from the keyboard 560 of a personal computer 50 with reference to drawing 16 (step S400), a controller 510 will transmit the Request to Send of authentication data to a memory card 110 through a portable telephone 100 (step S402). And the controller 1420 of a memory card 110 receives the Request to Send of authentication data through a terminal 1426, an interface 1424, and a bus BS 4 (step S404).

[0171] A controller 1420 will output read-out and its read authentication data {K_{Pm3}//C_{m3}} K_{Pa} for authentication data {K_{Pm3}//C_{m3}} K_{Pa} to the exterior through a bus BS 4, an interface 1424, and a terminal 1426 through a bus BS 4 from the authentication data-hold section 1400, if the Request to Send of authentication data is received (step S406). And the controller 510 of a personal computer 50 transmits authentication data {K_{Pm3}//C_{m3}} K_{Pa} for authentication data {K_{Pm3}//C_{m3}} K_{Pa} to the license management device 520 through a receipt and a bus BS 2 through a terminal 580 and the USB interface 550 (step S408).

[0172] If it does so, the controller 5220 of the license management device 520 will receive authentication data {K_{Pm3}//C_{m3}} K_{Pa} through a terminal 5226 and an interface 5224, and will give the authentication data {K_{Pm3}//C_{m3}} K_{Pa} which received to the decode processing section 5208 through a bus BS 5. And the decode processing section 5208 performs decode processing of authentication data {K_{Pm3}//C_{m3}} K_{Pa} with the authentication key K_{Pa} from the K_{Pa} attaching part 5214 (step S410). A controller 1420 performs authentication processing which judges whether the authentication data which gave the code for proving the justification in the engine of normal were received, in order to attest that whether processing having been performed normally and a memory card 110 hold the class public presentation cryptographic key K_{Pm3} and the class certificate C_{m3} from a memory card of normal from the decode processing result in the decode processing section 5208 (step S412). When it is

judged that it is just authentication data, a controller 5220 recognizes and receives the class public presentation cryptographic key $KPm3$ and the class certificate $Cm3$. And it shifts to the next processing (step S414). In not being just authentication data, it supposes un-recognizing, and it ends processing without receiving the class public presentation cryptographic key $KPm3$ and the class certificate $Cm3$ (step S478).

[0173] If it is checked as a result of authentication that it is access with just authentication data from a memory card, in the license management device 520, a controller 5220 will control the session key generating section 5218, and the session key generating section 5218 will generate session key $Ks2a$ for a loan (step S414). Session key $Ks2a$ is enciphered by the encryption processing section 5210 by the class public presentation cryptographic key $KPm3$ corresponding to the memory card 110 obtained by the decode processing section 5208. And a controller 5220 acquires encryption $\{Ks2data\ a\} Km3$ through a bus BS 5, and outputs encryption $\{Ks2data\ a\} Km3$ through a bus BS 5, an interface 5224, and a terminal 5226 (step S416).

[0174] A controller 510 receives $\{Ks2a\} Km3$ from a transmitting side through a bus BS 2 (step S418), and acquires the license ID corresponding to the license which performs the loan currently recorded on the license management information 530 of a transmitting side, i.e., HDD, (step S420). And a controller 510 uses the acquired license ID and encryption $\{Ks2data\ a\} Km3$ received in step S418 as data one, and transmits license ID// $\{Ks2a\} Km3$ to a memory card 110 through a terminal 580 and the USB interface 550 (step S422). If it does so, the controller 1420 of a memory card 110 will receive license ID// $\{Ks2a\} Km3$ through a terminal 1426, an interface 1424, and a bus BS 4 (step S424). Then, a controller 1420 gives encryption $\{Ks2data\ a\} Km3$ to the decode processing section 1422, and with the class secret decode key $Km3$ from the Km attaching part 1421, the decode processing section 1422 decodes $\{Ks2a\} Km3$, and receives session key $Ks2a$ (step S426). And the session key generating section 1418 generates session key $Ks2b$ (step S428), and the encryption processing section 1406 enciphers session key $Ks2b$ acquired by switching the terminal of a change-over switch 1446 one by one, and the individual public presentation cryptographic key $KPmc4$ by session key $Ks2a$ decoded by the decode processing section 1404, and it generates $Ks2b//\text{encryption}\{data\ KPmc\ 4\} Ks2a$. A controller 1420 outputs $Ks2b//\text{encryption}\{data\ KPmc\ 4\} Ks2a$ through a bus BS 4, an interface 1424, and a terminal 1426 (step S430), and a controller 510 receives $Ks2b//\text{encryption}\{data\ KPmc\ 4\} Ks2a$ through a terminal 580 and the USB interface 550. And a controller 510 inputs $Ks2b//\text{encryption}\{data\ KPmc\ 4\} Ks2a$ into the license management device 520 through a bus BS 2 (step S432).

[0175] If it does so, the controller 5220 of the license management device 520 will receive $Ks2b//\text{encryption}\{data\ KPmc\ 4\} Ks2a$ through a terminal 5226, an interface 5224, and a bus BS 5, and will give its $Ks2b//\text{encryption}\{data\ KPmc\ 4\} Ks2a$ which received to the decode processing section 5212. By session key $Ks2a$ from the session key generating section 5218,

the decode processing section 5212 decodes Ks2b//encryption {data KPmc 4} Ks2a, and receives session key Ks2b and the open cryptographic key KPmc4 (step S434).

[0176] Then, a controller 510 acquires the entry number in which the license set from the license management information corresponding to the license which lends out as the object of migration is stored (step S436). The license ID for a loan is generated (step S438). A loan demand of the license specified according to the license ID for a loan generated in the entry number and step S438 which were acquired in step S436 is inputted into the license management device 520 (step S440). The controller 5220 of the license management device 520 receives a loan demand of the license ID for an entry number and a loan, and a license through a terminal 5226, an interface 5224, and a bus BS 5, and acquires a license (License ID, content ID, the license key Kc, the access-control information ACm, playback control information ACp) from the entry of license field 5215A of the memory 1415 specified by the received entry number (step S442).

[0177] A controller 5220 judges whether the duplicate of a license is possible by the acquired access control ACm (step S444), if it can be reproduced, it will shift to step S452 of drawing 17, and if the duplicate is forbidden, it will shift to step S446 of drawing 17.

[0178] When judged with the duplicate of a license being forbidden in step S444 with reference to drawing 17, the loan propriety of the license acquired in step S442 is judged with a loan flag (step S446). And loan actuation will be ended if the acquired license cannot be lent out (step S478). If the acquired license can be lent out, a controller 5220 changes the loan flag in the specified entry "during a loan", stores the received license ID for a loan in the column of License ID at the time of a loan, and stores in the column of the loan place ID the open cryptographic key KPmc4 received in step S434 (step S448). And a controller 5220 generates the access-control information ACm for a loan (migration / duplicate control information is "3") that the ban on migration and a duplicate was set up, and permutes it by the license ID which acquired the license ID for a loan which received, and the generated access-control information ACm for a loan from the specified entry, and the access-control information ACm (step S450). While the license (the license ID for a loan, content ID, the license key Kc, the access-control information ACm for a loan, playback control information ACp) lent out to a memory card 110 is generated by this, the original license (the license ID for a loan, content ID, the license key Kc, the access-control information ACm for a loan, playback control information ACp) is stored in license field 5215A of the memory 5215 of the license management device 520. And a license of being stored in license field 5215A of the license management device 520 is lent out to a memory card 110. For this reason, in order that a license may remain unlike the case of migration, it functions on the license management device 520 as backup of a license.

[0179] When judged with a duplicate being possible in step S444, after step S450, the encryption processing section 5217 enciphers a license to the memory card 110 obtained by

the decode processing section 5212, and generates encryption data {license ID// content ID//Kc//ACm//ACp} Kmc4 by the open cryptographic key KPmc4 of a proper to it (step S452). In addition, when judged with the duplicate of a license being possible in step S444, the license acquired in step S442 is enciphered by the open cryptographic key KPmc4.

[0180] The encryption processing section 5206 minds the contact Pc of a switch 5246 for encryption data {license ID// content ID//Kc//ACm//ACp} Kmc4 enciphered by the encryption processing section 5217. And a receipt, A receipt and encryption data {license ID// content ID//Kc//ACm//ACp} Kmc4 are enciphered for session key Ks2b decoded by the decode processing section 5212 with session key Ks2b through the contact Pb of a switch 5242. And a controller 5220 outputs encryption data {{license ID// content ID//Kc//ACm//ACp} Kmc4} Ks2b through a bus BS 5, an interface 5224, and a terminal 5226 (step S454).

[0181] A controller 510 receives encryption data {{license ID// content ID//Kc//ACm//ACp} Kmc4} Ks2b from a memory card 120 through a bus BS 2, and inputs it into the memory card 110 of the loan place equipped with the received encryption data {{license ID// content ID//Kc//ACm//ACp} Kmc4} Ks2b by the portable telephone 100 (step S456).

[0182] The controller 1420 of a memory card 110 gives encryption data {{license ID// content ID//Kc//ACm//ACp} Kmc4} Ks2b to the decode processing section 1412 in response to the input of encryption data {{license ID// content ID//Kc//ACm//ACp} Kmc4} Ks2b through a terminal 1426, an interface 1424, and a bus BS 4. And the decode processing section 1412 decodes encryption data {{license ID// content ID//Kc//ACm//ACp} Kmc4} Ks2b with session key Ks2b generated by the receipt and the session key generating section 1418 through the bus BS 4, and receives {license ID// content ID//Kc//ACm//ACp} Kmc4 (step S458).

[0183] Then, encryption data {license ID// content ID//Kc//ACm//ACp} Kmc4 is decoded by directions of a controller 1420 with the secret decode key Kmc4 in the decode processing section 1404, and a license (the license key Kc, License ID, content ID, the access-control information ACm, and playback control information ACp) is received by them (step S460).

[0184] If it does so, while a controller 510 will determine the entry number for storing the license moved / reproduced from the license management information of the memory card 110 which is a receiving side and will input it into a memory card 110, the license management information of a receiving side is updated (step S462).

[0185] If it does so, it will judge whether the controller 1420 of a memory card 100 can lend out the acquired license based on the access-control information ACm acquired in step S460 (step S464). And if the loan of a license is possible for a controller 1420, the loan flag stored in the field specified by the entry number of license field 1415A of memory 1415 will be set as "good" (step S466). On the other hand, in step S360, when judged with the loan of a license being impossible, a controller 1420 sets as "improper" the loan flag stored in the field specified by the entry number of license field 1415A (step S468). In a loan, since migration / duplicate control information of access-control information is set up improper [migration and

a duplicate] and is outputted from the license management device 520 in step S450, it surely progresses to step S468.

[0186] A controller 1420 after step S466 or step S468 The effective flag stored in the field specified by the entry number of license field 1415A is set as "effective" (step S470). The license (License ID, content ID, the license key Kc, the access-control information ACm, and playback control information ACp) received in step S460 to the field specified by the entry number of license field 1415A is stored (step S472).

[0187] On the other hand, it judges whether migration or the duplicate of a license is possible for a controller 510 after step S462 (step S474), and when movable, the license ID for a loan is added to the license management information of a loan place, and loan place license management information is updated (step S476). In step S474, when judged with the loan of a license being possible, loan actuation of a license is ended after step S476 or step S472 (step S478).

[0188] In addition, what is necessary is just to perform the loan to the memory card 110 of encryption contents data by a controller's 510 reading encryption contents data from HDD530, and transmitting to a memory card 110, after migration of a license is completed.

[0189] Thus, after checking that the open cryptographic key KPm3 which has enciphered and transmitted to that the memory card 110 with which the portable telephone 100 was equipped is the device of normal, and coincidence with the class certificate Cm3 is effective, a license can be lent out only to the loan demand to a regular memory card, and the loan to an inaccurate memory card can be forbidden.

[0190] Moreover, by exchanging the cryptographic key generated by the memory card, performing encryption using the cryptographic key which each received, and transmitting the encryption data to the other party, de facto mutual recognition can be performed also in transmission and reception of each encryption data, and the security in loan actuation of a license can be raised.

[0191] The actuation which returns the license lent out to the memory card 110 from the license management device 520 explained with reference to [return] drawing 16 and drawing 17 from a memory card 110 to the license management device 520 is explained.

[0192] Drawing 18 - drawing 21 are the 1st for explaining the actuation which returns a license to the license management device 520 from a memory card 110 - the 4th flow chart.

[0193] In addition, before the processing in drawing 18 , a user determines the license and contents which are returned from the memory card 110 with which the portable telephone 100 connected to the personal computer 50 by the USB cable 70 was equipped according to the contents list file currently recorded on HDD530, and explains as a premise that the license management file of the both sides by the side of the contents file by the side of return, a loan, and return can be specified.

[0194] If a return request is inputted from the keyboard 560 of a personal computer 50 with

reference to drawing 18 (step S500), a controller 510 will transmit the Request to Send of authentication data to a memory card 110 through a terminal 580 and the USB interface 550 (step S502). And the controller 1420 of a memory card 110 receives the Request to Send of authentication data through a terminal 1426, an interface 1424, and a bus BS 4 (step S504).

[0195] A controller 1420 will output read-out and its read authentication data {K_{Pm3}//C_{m3}} K_{Pa} for authentication data {K_{Pm3}//C_{m3}} K_{Pa} to a controller 510 through a bus BS 4, an interface 1424, and a terminal 1426 through a bus BS 4 from the authentication data-hold section 1400, if the Request to Send of authentication data is received (step S506). And a controller 510 transmits authentication data {K_{Pm3}//C_{m3}} K_{Pa} for authentication data {K_{Pm3}//C_{m3}} K_{Pa} to the license management device 520 through a receipt and a bus BS 2 through a terminal 580 and the USB interface 550 (step S508).

[0196] If it does so, the controller 5220 of the license management device 520 will receive authentication data {K_{Pm3}//C_{m3}} K_{Pa} through a terminal 5226 and an interface 5224, and will give the authentication data {K_{Pm3}//C_{m3}} K_{Pa} which received to the decode processing section 5208 through a bus BS 5. And the decode processing section 5208 performs decode processing of authentication data {K_{Pm3}//C_{m3}} K_{Pa} with the authentication key K_{Pa} from the K_{Pa} attaching part 5214 (step S510). A controller 5220 performs authentication processing which judges whether the authentication data which gave the code for proving the justification in the engine of normal were received, in order to attest that whether processing having been performed normally and a memory card 110 hold the class public presentation cryptographic key K_{Pm3} and the class certificate C_{m3} from a memory card of normal from the decode processing result in the decode processing section 5208 (step S512). When it is judged that it is just authentication data, a controller 5220 recognizes and receives the class public presentation cryptographic key K_{Pm3} and the class certificate C_{m3}. And it shifts to the next processing (step S514). In not being just authentication data, it supposes un-recognizing, and it ends processing without receiving the class public presentation cryptographic key K_{Pm3} and the class certificate C_{m3} (step S638).

[0197] If it is checked that it is access from the playback terminal equipped with a memory card with just authentication data as a result of authentication, in the license management device 520, a controller 5220 will control the session key generating section 5218, and the session key generating section 5218 will generate session key K_{s2a} for return (step S514). Session key K_{s2a} is enciphered by the encryption processing section 1410 by the class public presentation cryptographic key K_{Pm3} corresponding to the memory card 110 obtained by the decode processing section 5208. And a controller 5220 acquires encryption {K_{s2data} a} K_{m3} through a bus BS 5, and outputs encryption {K_{s2data} a} K_{m3} through a bus BS 5, an interface 5224, and a terminal 5226 (step S516).

[0198] A controller 510 receives {K_{s2a}} K_{m3} from the license management device 520 through a bus BS 2 (step S518), and acquires the license ID at the time of a loan from the

license management information of a lending out agency (step S520). And a controller 40 uses the acquired license ID and encryption {Ks2data a} Km3 received in step S518 as data one, and transmits license ID//{Ks2a} Km3 to a memory card 110 (step S522). If it does so, the controller 1420 of a memory card 110 will receive license ID//{Ks2a} Km3 through a terminal 1426, an interface 1424, and a bus BS 4 (step S524). Then, a controller 1420 gives encryption {Ks2data a} Km3 to the decode processing section 1422, and with the class secret decode key Km3 from the Km attaching part 1421, the decode processing section 1422 decodes {Ks2a} Km3, and receives session key Ks2a (step S526). And the session key generating section 1418 generates session key Ks2b (step S528), and the encryption processing section 1406 enciphers session key Ks2b acquired by switching the terminal of a change-over switch 1446 one by one, and the individual public presentation cryptographic key KPmc4 by session key Ks2a decoded by the decode processing section 1404, and it generates Ks2b//encryption {data KPmc 4} Ks2a. A controller 1420 outputs Ks2b//encryption {data KPmc 4} Ks2a through a bus BS 4, an interface 1424, and a terminal 1426 (step S530), and a controller 510 receives Ks2b//encryption {data KPmc 4} Ks2a through a terminal 580 and the USB interface 550. And a controller 510 transmits Ks2b//encryption {data KPmc 4} Ks2a to the license management device 520 through a bus BS 2 (step S532).

[0199] If it does so, the controller 5220 of the license management device 520 will receive Ks2b//encryption {data KPmc 4} Ks2a through a terminal 5226, an interface 5224, and a bus BS 5, and will give its Ks2b// encryption {data KPmc 4} Ks2a which received to the decode processing section 5212. By session key Ks2a from the session key generating section 5218, the decode processing section 5212 decodes Ks2b//encryption {data KPmc 4} Ks2a, and receives session key Ks2b and the open cryptographic key KPmc4 (step S534).

[0200] And a controller 510 inputs a retrieval demand of a license into the memory card 110 of a loan place (step S534). The controller 1420 of a memory card 110 searches license field 1415A of memory 1415 based on the license ID which received the retrieval demand of a license through the terminal 1426, the interface 1424, and the bus BS 4 (step S536), and was received in step S524. And a controller 1420 generates the retrieval result state (step S538).

[0201] The encryption processing section 1406 receives session key Ks2a decoded and obtained by the decode processing section 1412 through the contact Pb of a switch 1442, and receives session key Ks2b which the session key generating section 1418 generated through the contact Pd of a switch 1446. And the encryption processing section 1406 enciphers session key Ks2b by session key Ks2a, and generates encryption data {Ks2b} Ks2a (step S540). And a controller 1420 generates license ID//{Ks2b} Ks2a//state, and calculates hash value hash of the generated license ID//{Ks2b} Ks2a//state (step S542). That is, a controller 1420 signs license ID//{Ks2b} Ks2a//state. Then, a controller 1420 gives hash value hash to the encryption processing section 1406 through the contact Pf of a switch 1446. The encryption processing section 1406 enciphers hash value hash by session key Ks2a, and generates

encryption {data hash} Ks2a (step S544).

[0202] With reference to drawing 19 , the controller 1420 of a memory card 110 generates license ID//{Ks2b} Ks2a//state//{hash} Ks2a, and outputs license ID//{Ks2b} Ks2a//state//{hash} Ks2a through a bus BS 4, an interface 1424, and a terminal 1426 (step S546). A controller 510 receives license ID//{Ks2b} Ks2a//state//{hash} Ks2a from a memory card 110 through a terminal 580 and the USB interface 550 (step S548). and -- a controller -- 510 -- a loan -- origin -- a license -- management information -- from -- returning -- a license -- storing -- having -- **** -- an entry -- a number -- acquiring (step S550) -- a step -- S -- 548 -- setting -- having acquired -- a license -- ID -- /- /- {- Ks -- 2b --} -- Ks -- two -- a -- /- /- state -- /- /- {- hash --} -- Ks -- two -- a -- an entry -- a number -- having specified -- a license -- return -- a demand -- a loan -- origin -- a license -- management -- a device -- 520 -- inputting (step S552) . The controller 5220 of the license management device 520 License ID//{Ks2b} Ks2a//state//{hash} Ks2a, an entry number, and a license return demand are received through a terminal 5226, an interface 5224, and a bus BS 5 (step S554). The open cryptographic key KPmcx stored in the license ID at the time of the loan flag stored in the field specified by the received entry number and a loan and the loan place ID is acquired (step S556).

[0203] If it does so, a controller 5220 judges whether it is in agreement with the memory card 110 which the acquired open cryptographic key KPmcx received in step S534 at the open cryptographic key KPmc4 of a proper (step S558), and when inharmonious, it will end return actuation (step S638). That is, since it means that it judged that a memory card 110 is not the partner who lent out the license, return actuation will be ended. Since it is not necessary to return a license if it judges whether the controller 5220 has become while a loan flag lends out (step S560) and is not [be / it] under loan when the open cryptographic key KPmcx is in agreement with the open cryptographic key KPmc4, return actuation is ended (step S638). If judged with a license returning in step S560, a controller 5220 judges whether the received license ID is in agreement with the license ID at the time of a loan (step S562), and when inharmonious, it will end return actuation (step S638). That is, since it will not be in agreement with the license ID of the license which the license ID of the license with a return demand lent out and the lent-out license will be returned, return actuation will be ended. In step S562, when two licenses ID are in agreement, a controller 5220 checks the retrieval result state of the license in a memory card 110 (step S564). That is, when the license which is going to return a controller 5220 checks whether it is truly stored in license field 1415A of a memory card 110 and is not stored in license field 1415A, it ends return actuation (step S638). And a controller 5220 calculates hash value hash of license ID//{Ks2b} Ks2a//state, when it checks that the license which it is going to return is stored in license field 1415A of a memory card 110 (step S566). That is, the controller 5220 of the license management device 520 performs the signature to license ID//{Ks2b} Ks2a//state itself, and calculates hash value

hash.

[0204] Then, a controller 5220 gives {hash} Ks2a received in step S554 to the decode processing section 5212. The decode processing section 5212 decodes {hash} Ks2a by session key Ks2a, and a controller 5220 receives hash value hash in a memory card 110 (step S568). And it judges whether hash value hash of a controller 5220 calculated itself corresponds with hash value hash in a memory card 110 (step S570), and when inharmonious, since the signature in a memory card 110 will be rewritten, return actuation is ended (step S638). When two hash values are in agreement, a controller 5220 gives encryption data {Ks2b} Ks2a received in step S554 to the decode processing section 5212. The decode processing section 5212 decodes encryption data {Ks2b} Ks2a by session key Ks2a, and receives session key Ks2b (step S572).

[0205] And a controller 5220 checks session key Ks2b (step S574), and if inharmonious and it is [return actuation is ended (step S638) and] in agreement with session key Ks2b received from the memory card 110 at the time of the loan of a license, it will shift to step S576 of drawing 20 .

[0206] The invalid dummy license for making into an invalid the license lent out to the loan place with reference to drawing 20 (the fake license ID, fake content ID, the fake license key Kc, the fake access-control information ACm, and the fake playback control information ACp are generated, and the generated invalid dummy license is given to the encryption processing section 5217.) The encryption processing section 5217 enciphers an invalid dummy license by the open cryptographic key KPMC4 decoded by the decode processing section 5212, and generates fake license ID// fake content ID// fake license key Kc/the /fake access-control information ACm/encryption data {/fake playback control information ACp} Kmc4 (step S576). The encryption processing section 5206 minds the contact Pc of a switch 5246 for fake license ID// fake content ID// fake license key Kc/the /fake access-control information ACm/encryption data {/fake playback control information ACp} Kmc4. And a receipt, The received encryption data {fake license ID// fake content ID// fake license key Kc/the /fake access-control information ACm/the /fake playback control information ACp} The contact Pd of a switch 5246 is minded for Kmc4. It enciphers with received session key Ks2b, and encryption data {fake license ID// fake content ID// fake license key Kc/fake access-control information ACm/{/fake playback control information ACp} Kmc4} Ks2b is outputted. And a controller 5220 outputs encryption data {fake license ID// fake content ID// fake license key Kc/fake access-control information ACm/{/fake playback control information ACp} Kmc4} Ks2b through a bus BS 5, an interface 5224, and a terminal 5226 (step S578).

[0207] A controller 510 receives encryption data {fake license ID// fake content ID// fake license key Kc/fake access-control information ACm/{/fake playback control information ACp} Kmc4} Ks2b from the license management device 520 which is a lending out agency through a bus BS 2. Encryption data {fake license ID// fake content ID// fake license key

Kc//fake access-control information ACm/{/fake playback control information ACp} Kmc4} Ks2b is transmitted to the memory card 110 which is a loan place (step S580).

[0208] The controller 1420 of a memory card 110 receives encryption data {fake license ID// fake content ID// fake license key Kc//fake access-control information ACm/{/fake playback control information ACp} Kmc4} Ks2b through a terminal 1426, an interface 1424, and a bus BS 4, and gives the received encryption data to the decode processing section 1412. The decode processing section 1412 decodes encryption data with session key Ks2b, and receives fake license ID// fake content ID// fake license key Kc/the /fake access-control information ACm/{/fake playback control information ACp} Kmc4 (step S582). And the decode processing section 1404 Fake license ID// fake content ID// fake license key Kc/the /fake access-control information ACm/encryption data {/fake playback control information ACp} Kmc4 from the decode processing section 1412 with the private key Kmc4 from the Kmc attaching part 1402 It decodes and an invalid dummy license (fake license ID// fake content ID// fake license key Kc/the /fake access-control information ACm//fake playback control information ACp) is received (step S584).

[0209] If it does so, a controller 510 will acquire the entry number in which the license returned from the license management information of the memory card 110 which is a loan place is stored, and will transmit the acquired entry number to a loan place (step S586). It judges whether the loan of a license by the fake access control ACm is possible for the controller 1420 of a memory card 110 (step S588), if a loan is good, the loan flag of a license field will be set as "good" (step S590), and if a loan is improper, a loan flag will be set as "improper" (step S592). A controller 1420 sets the effective flag of license field 1415A specified by the entry number as "effective" after step S590 or step S592 (step S694), and a license (License ID, content ID, the license key Kc, access-control information, and count control information of playback) is stored in the field specified by the entry number (step S596). Since processing of steps S588, S590, S592, S594, and S596 is made common with "distribution" and "migration" which were mentioned above, although it is processed, since the fake access-control information ACm is always the ban on a migration duplicate, it is surely judged a loan is "impossible" in step S588, and progresses to step S592.

[0210] Then, a controller 510 inputs a retrieval demand of a license into a loan place again (step S598), and the controller 1420 of a memory card 110 receives the retrieval result of a license through a terminal 1426, an interface 1424, and a bus BS 4 (step S600). A controller 1420 searches license field 1415A of memory 1415 based on License ID. And a controller 1420 generates the retrieval result state (step S602).

[0211] The encryption processing section 1406 receives session key Ks2a decoded and obtained by the decode processing section 1412 through the contact Pb of a switch 1442, and receives session key Ks2b which the session key generating section 1418 generated through the contact Pd of a switch 1446. And the encryption processing section 1406 enciphers session

key Ks2b by session key Ks2a, and generates encryption data {Ks2b} Ks2a (step S604). And a controller 1420 generates license ID//{Ks2b} Ks2a//state, and calculates hash value hash of the generated license ID//{Ks2b} Ks2a//state (step S606). That is, a controller 1420 signs license ID//{Ks2b} Ks2a//state. Then, a controller 1420 gives hash value hash to the encryption processing section 1406 through the contact Pf of a switch 1446. The encryption processing section 1406 enciphers hash value hash by session key Ks2a, and generates encryption {data hash} Ks2a (step S608).

[0212] With reference to drawing 21, the controller 1420 of a memory card 110 generates license ID//{Ks2b} Ks2a//state//{hash} Ks2a, and outputs license ID//{Ks2b} Ks2a//state//{hash} Ks2a through a bus BS 4, an interface 1424, and a terminal 1426 (step S610). A controller 510 receives license ID//{Ks2b} Ks2a//state//{hash} Ks2a from a memory card 110 through a terminal 580 and the USB interface 550 (step S612). And a controller 510 inputs the license return acknowledge request which specified license ID//{Ks2b} Ks2a//state//{hash} Ks2a and an entry number into the license management device 520 which is a lending out agency through a bus BS 2 (step S614).

[0213] The controller 5220 of the license management device 520 receives license ID//{Ks2b} Ks2a//state//{hash} Ks2a, an entry number, and a license return acknowledge request through a terminal 5226, an interface 5224, and a bus BS 2 (step S616). And a controller 5220 judges whether the received license ID is in agreement with the license ID at the time of a loan (step S618), and if inharmonious, it will end return actuation (step S638). And in step S618, when judged with two licenses ID being in agreement, a controller 5220 checks the retrieval result state of the license in a memory card 110 (step S620). That is, return actuation is ended, when it checks whether the controller 5220 is eliminated truly [the license which it is going to return] from license field 1415A of a memory card 110 and a license exists in license field 1415A (step S638). And a controller 5220 calculates hash value hash of license ID//{Ks2b} Ks2a//state, when it checks that the license which it is going to return is eliminated from license field 1415A of a memory card 110 (step S622). That is, the controller 5220 of the license management device 520 performs the signature to license ID//{Ks2b} Ks2a//state itself, and calculates hash value hash.

[0214] Then, a controller 5220 gives {hash} Ks2a received in step S554 to the decode processing section 5212. The decode processing section 5212 decodes {hash} Ks2a by session key Ks2a, and a controller 5220 receives hash value hash in a memory card 110 (step S624). And it judges whether hash value hash of a controller 5220 calculated itself corresponds with hash value hash in a memory card 110 (step S626), and when inharmonious, since the signature in a memory card 110 will be rewritten, return actuation is ended (step S638). When two hash values are in agreement, a controller 5220 gives encryption data {Ks2b} Ks2a received in step S616 to the decode processing section 5212. The decode processing section 5212 decodes encryption data {Ks2b} Ks2a by session key Ks2a, and receives session key

Ks2b (step S628).

[0215] And a controller 5220 checks session key Ks2b (step S630), and with session key Ks2b received from the memory card 110 at the time of the loan of a license, if inharmonious, it will end return actuation (step S638). When two session key Ks2bs are in agreement in step S630, a controller 1420 changes the loan flag in the entry specified by the entry number into "it is good" (step S632). And a controller 40 deletes the information on the returned license, and updates the license management information and the playback list file which are recorded on data area 1415B of the memory card 110 of a loan place, and return actuation ends it (step S638).

[0216] Thus, encryption contents data can be reproduced and enjoyed in a portable telephone 100 and the playback terminal 102, leaving a license to the license management device 520 by returning and getting encryption contents data and a license from the phase hand who lent out encryption contents data and a license.

[0217] Moreover, since the license lent out to the memory card is specified that it cannot output the license which checked out the memory card to other record devices (a memory card, a license management device, and license administrative module) using the access-control information ACm, the lent-out license does not flow out. By checking in to the lent-out license administrative module (return), the right of the lent-out license returns to the lent-out license management device. Therefore, a duplicate is not allowed to be made against an author's mind, it is not the processing to which security level falls, and copyright is also protected.

[0218] With reference to drawing 22, management of the encryption contents data received by the license administrative module 511 or the license management device 520 of a personal computer 50 and a license is explained. HDD530 of a personal computer 50 includes the contents list file 150, the contents files 1531-1535, and the license management files 1521-1525.

[0219] The contents list file 150 is a data file of the list format of the contents to own, and the information (file name) which shows each information (musical piece name, artist name, etc.) over contents, and a contents file and a license management file is included. The information over each contents acquires information required from additional information Dc-inf at the time of reception, and is automatically indicated by directions of a user. Moreover, only a contents file can be managed in a list also about the contents which cannot reproduce only a license management file.

[0220] The contents files 1531-1535 are files which record encryption contents data {Dc} Kc received by the license administrative module 511 or the license management device 520, and additional information Dc-inf, and are prepared for every contents.

[0221] Moreover, the license management files 1521-1525 are files for managing the license which is recorded corresponding to the contents files 1531-1535, and was received by the

license administrative module 511 or the license management device 520, respectively. A license cannot usually be referred to so that clearly [old explanation], but if other information except the license key Kc cannot even perform that a user rewrites, it is satisfactory in respect of protection of copyrights. However, since it leads to the fall of security, it is not desirable to dissociate with the license key Kc and to manage in employment. Then, when receiving license distribution, the counterpart of the matter restricted by the transaction ID which can be referred to in a plaintext, content ID, and the access-control information ACm and the playback control information ACp which can be easily judged from the license purchase conditions AC, and record of check-out are recorded in a plaintext. Furthermore, an entry number is recorded when a license is recorded on the license management device 520.

[0222] The license management files 1521, 1522, 1524, and 1525 contain the entry numbers 0, 2, 1, and 3, respectively. This is a number which specifies the management domain of the license (License ID, the license key Kc, the access-control information ACm, and playback control information ACm) which is received by the license management device 520 and managed in license field 5215A of the memory 5215 of the license management device 520.

[0223] Moreover, it is a solution or ** where if the contents files 1531-1535 are searched and the contents file 1531 is extracted when moving the encryption contents data of the file name recorded on the contents file 1531 to the memory card 110 equipped by the portable telephone 100 or the playback terminal 102, the license which reproduces encryption contents data is managed. Since the entry number contained in the license management file 1521 corresponding to the contents file 1531 is "0", the license which reproduces the encryption contents data of the file name recorded on the contents file 1531 is recorded on the field specified by the entry number 0 of license field 5215A of the memory 5215 of the license management device 520. If it does so, a license is easily movable to drawing and a memory card 110 from license field 5215A of memory 5215 by inputting the entry number 0 into read-out from the license management file 1521 of the contents list file 150 recorded on HDD530, and inputting the read entry number 0 into the license management device 520. And since the effective flag in the entry number specified in license field 5215A of memory 5215 is made into an "invalid" after moving a license (step S346 reference of drawing 15), corresponding to it, "nothing [license]" is recorded like the license management file 1523.

[0224] The license management file 1523 contains "nothing [license]." This is the result of moving the license received by the license management device 520. The corresponding contents file 1533 remains recorded on HDD530. It is possible to receive distribution from a memory card only about a license, when distribution is again licensed from migration or the distribution server 10 to the license administrative module 520.

[0225] In a loan and return, an entry number can be specified and processed similarly. Moreover, in a loan, a license management file records the license ID at the time of a loan for

the media ID assigned to the information for specifying the existence and the loan place of a loan, for example, a memory card. Such information is eliminated at the time of return.

[0226] Thus, in this invention, encryption contents data can be freely reproduced with a portable telephone 100 or the playback terminal 102, protecting copyright, without reducing security level, leaving the license currently recorded on the license management device 520 to the license management device 520.

[0227] Drawing 23 shows license field 1415A and data area 1415B in memory 1415 of a memory card 110. The playback list file 160, the contents files 1611-161n, and the license management files 1621-162n are recorded on data area 1415B. The contents files 1611-161n record encryption contents data {Dc} Kc and additional information Dc-inf which received as one file. Moreover, the license management files 1621-162n are recorded corresponding to the contents files 1611-161n, respectively. It is [that each data currently recorded on HDD530 in a personal computer 50 is only recorded on data area 1415B of the memory 1415 of a memory card 110, and], and other points are the same as drawing 22 .

[0228] Moreover, although the license management file 1622 is shown by the dotted line, it shows what is not recorded in fact. Although it means that there is no license and it cannot be reproduced although the contents file 1612 exists, this corresponds, when for example, a playback terminal receives only encryption contents data from other portable telephones.

[0229] Moreover, the contents file 1613 means that encryption contents data do not exist, although it corresponds when for example, a playback terminal receives encryption contents data and a license from the distribution server 10 and this transmits only the received encryption contents data to a personal computer 50, although shown by the dotted line, and a license exists in memory 1415.

[0230] In addition, license management domain 1415A has the same composition as license management domain 5215A of a license management device. therefore, other memory cards [memory card / 110] -- lending out -- further -- the license management device 520 -- also lending out -- it is possible.

[0231] As [playback] **** was carried out, the memory card 110 with which the portable telephone 100 or the playback terminal 102 was equipped can receive encryption contents data and a license directly from the distribution server 10. Moreover, a memory card 110 can receive the encryption contents data and the license which the personal computer 50 acquired from the distribution server 10 in hard from a personal computer 50 by the concept of "migration." Furthermore, a memory card 110 can receive the encryption contents data and the license which the personal computer 50 acquired from the distribution server 10 or Music CD in software from a personal computer 50 by the concept of "a loan."

[0232] Thus, a memory card 110 receives encryption contents data and a license by various kinds of approaches. Then, playback of the encryption contents data which the memory card received by these approaches of various kinds of is explained below.

[0233] Drawing 24 is a flow chart for explaining the playback actuation in the playback terminal 102 of the contents data which the memory card 110 received. In addition, before the processing in drawing 24, according to the playback list currently recorded on data area 1415B of a memory card 100, the user of the playback terminal 102 determines the contents (musical piece) to reproduce, specifies a contents file, and explains acquiring the license management file as a premise.

[0234] With reference to drawing 24, a playback request is inputted to the playback terminal 100 through a control panel 1108 with initiation of playback actuation from the user of the playback terminal 100 (step S700). If it does so, a controller 1106 will perform the output request of authentication data to the contents regenerative circuit 1550 through a bus BS 3 (step S702), and the contents regenerative circuit 1550 will receive the output request of authentication data (step S704). And the authentication data-hold section 1500 outputs authentication data {KPp1//Cp1} KPp1 (step S706), and a controller 1106 inputs authentication data {KPp1//Cp1} KPp1 into a memory card 110 through the memory card interface 1200 (step S708).

[0235] If it does so, a memory card 110 receives authentication data {KPp1//Cp1} KPp1, the decode processing section 1408 will decode received authentication data {KPp1//Cp1} KPp1 with the open authentication key KPp1 held at the KPp1 attaching part 1414 (step S710), and a controller 1420 will perform authentication processing from the decode processing result in the decode processing section 1408. That is, authentication processing which judges whether authentication data {KPp1//Cp1} KPp1 is authentication data of normal is performed (step S712). When it is not able to decode, it shifts to step S748 and playback actuation is ended. When authentication data are able to be decoded, a controller 1420 controls the session key generating section 1418, and the session key generating section 1418 generates the session key Ks2 for playback sessions (step S714). And the cipher-processing section 1410 outputs {Ks2} Kp1 which enciphered the session key Ks2 from the session key generating section 1418 by the open cryptographic key KPp1 decoded in the decode processing section 1408 to a bus BS 3. If it does so, a controller 1420 will output {Ks2} Kp1 to the memory card interface 1200 through an interface 1424 and a terminal 1426 (step S716). The controller 1106 of the playback terminal 100 acquires {Ks2} Kp1 through the memory card interface 1200. And a controller 1106 gives {Ks2} Kp1 to the decode processing section 1504 of the contents regenerative circuit 1550 through a bus BS 3 (step S718), and the decode processing section 1504 decodes {Ks2} Kp1 with the secret decode key Kp1 which was outputted from KPp1 attaching part 1502 and which is the open cryptographic key KPp1 and a pair, and it outputs the session key Ks2 to the cipher-processing section 1506 (step S720). If it does so, the session key generating section 1508 will generate the session key Ks3 for playback sessions, and will output the session key Ks3 to the cipher-processing section 1506 (step S722). The cipher-processing section 1506 enciphers the session key Ks3 from the session key generating

section 1508 by the session key Ks2 from the decode processing section 1504, and outputs {Ks3} Ks2 (step S724), and a controller 1106 outputs {Ks3} Ks2 to a memory card 110 through a bus BS 3 and the memory card interface 1200 (step S726).

[0236] If it does so, the decode processing section 1412 of a memory card 110 will input {Ks3} Ks2 through a terminal 1426, an interface 1424, and a bus BS 4. The decode processing section 1412 decodes {Ks3} Ks2 by the session key Ks2 generated by the session key generating section 1418, and receives the session key Ks3 generated at the playback terminal 100 (step S728).

[0237] The controller 1106 of a playback terminal outputs the output request of the entry number which acquired the entry number in which the license is stored from the license management file of the playback request song beforehand acquired from the memory card 110 (step S730), and was acquired to the memory card 110 through the memory card interface 1200, and a license (step S732).

[0238] The controller 1420 of a memory card 110 receives an entry number and the output request of a license, and acquires the license stored in the field specified by the entry number (step S734).

[0239] And a controller 1420 checks the access-restriction information ACm (step S736).

[0240] It ends playback actuation, in being in a condition [that it is already unreproducible], and when the count of playback of access-restriction information has a limit, after changing the count of playback of the access-restriction information ACm (step S738), in step S736, it specifically progresses to the following step (step S740) by checking the count of playback by checking the access-restriction information ACm which is the information about the limit to access of memory. On the other hand, when playback is not restricted by the count of playback of the access-restriction information ACm, step S738 is skipped, and processing advances to the following step (step S740), without changing the count of playback of the access-restriction information ACm.

[0241] In step S736, when it is judged in the playback actuation concerned that it is reproducible, the license key Kc and the playback control information ACp of a playback request song which were recorded on license field 1415A of memory 1415 are outputted on a bus BS 4 (step S740).

[0242] The license key Kc and the playback control information ACp which were acquired are sent to the encryption processing section 1406 through the contact Pf of a change-over switch 1446. The encryption processing section 1406 enciphers the license key Kc which won popularity through the change-over switch 1446 by the session key Ks3 received from the decode processing section 1412 through the contact Pb of a change-over switch 1442, and the playback control information ACp, and outputs {Kc//ACp} Ks3 to a bus BS 4 (step S740).

[0243] The encryption data outputted to the bus BS 4 are sent out to the playback terminal 102 through an interface 1424, a terminal 1426, and the memory card interface 1200.

[0244] In the playback terminal 102, the decode processing section 1510 performs decode processing for encryption data {Kc//ACp} Ks3 transmitted to a bus BS 3 through the memory card interface 1200, and the license key Kc and the playback control information ACp are received (steps S742 and S744). The decode processing section 1510 transmits the license key Kc to the decode processing section 1516, and outputs the playback control information ACp to a bus BS 3.

[0245] Through a bus BS 3, a controller 1106 receives the playback control information ACp, and checks reproductive propriety (step S746).

[0246] In step S746, when it is judged by the playback control information ACp that playback is impossible, playback actuation is ended.

[0247] When it is judged in step S746 that it is refreshable, a controller 1106 requires encryption contents data {Dc} Kc of a memory card 110 through the memory card interface 1200. If it does so, the controller 1420 of a memory card 110 will acquire encryption contents data {Dc} Kc from memory 1415, and will output it to the memory card interface 1200 through a bus BS 4, an interface 1424, and a terminal 1426.

[0248] The controller 1106 of the playback terminal 102 acquires encryption contents data {Dc} Kc through the memory card interface 1200, and gives encryption contents data {Dc} Kc to the contents regenerative circuit 1550 through a bus BS 3.

[0249] And the decode processing section 1516 of the contents regenerative circuit 1550 decodes encryption contents data {Dc} Kc with the license key Kc outputted from the decode processing section 1510, and acquires the contents data Dc.

[0250] And they are outputted to the music playback section 1518, and the decoded contents data Dc reproduce contents data, and the music playback section 1518 changes a digital signal into an analog signal, and outputs DA converter 1519 to a terminal 1530. And from a terminal 1530, through an external output unit, music data are outputted to a head telephone 130, and are reproduced. Playback actuation is completed by this (step S748).

[0251] Since the flag it is shown that the memory card of a lending out agency manages the lent-out license according to License ID at the time of the loan place ID and a loan, the loan of a license manages with a loan flag, it generates from the license whose self held the license for a loan at the time of the loan of a license, and the original license is under loan sets up to a loan flag according to the gestalt of operation of this invention, backup of the license lent out can provide.

[0252] It should be thought that the gestalt of the operation indicated this time is [no] instantiation at points, and restrictive. The range of this invention is shown by the above-mentioned not explanation but claim of the gestalt of operation, and it is meant that all modification in a claim, equal semantics, and within the limits is included.

[0253]

[Effect of the Invention] Since the flag it is shown that the memory card of a lending out

agency manages the lent-out license according to License ID at the time of the loan place ID and a loan, the loan of a license is managed with a loan flag, it generates from the license whose self held the license for a loan at the time of the loan of a license, and the original license is under loan sets up to a loan flag according to this invention, backup of the license lent out can provide.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the schematic diagram which explains a data distribution system notionally.

[Drawing 2] It is the schematic diagram which explains other data distribution systems notionally.

[Drawing 3] It is drawing showing properties, such as data for the communication link in the data distribution system shown in drawing 1 and drawing 2 , and information.

[Drawing 4] It is drawing showing properties, such as data for the communication link in the data distribution system shown in drawing 1 and drawing 2 , and information.

[Drawing 5] It is the outline block diagram showing the configuration of the distribution server in the data distribution system shown in drawing 1 and drawing 2 .

[Drawing 6] It is the outline block diagram showing the configuration of the personal computer in the data distribution system shown in drawing 1 and drawing 2 .

[Drawing 7] It is the outline block diagram showing the configuration of the playback terminal in the data distribution system shown in drawing 2 .

[Drawing 8] It is the outline block diagram showing the configuration of the memory card in the data distribution system shown in drawing 1 and drawing 2 .

[Drawing 9] It is the outline block diagram showing the configuration of the license management device shown in drawing 6 .

[Drawing 10] It is the 1st flow chart for explaining the distribution actuation in the data distribution system shown in drawing 1 and drawing 2 .

[Drawing 11] It is the 2nd flow chart for explaining the distribution actuation in the data distribution system shown in drawing 1 and drawing 2 .

[Drawing 12] It is a functional block diagram for explaining the function of software to perform ripping.

[Drawing 13] It is a flow chart for explaining actuation of ripping in the data distribution system shown in drawing 1 and drawing 2 .

[Drawing 14] It is the 1st flow chart for explaining migration actuation of a license of the encryption contents data in the data distribution system shown in drawing 1 and drawing 2 .

[Drawing 15] It is the 2nd flow chart for explaining migration actuation of a license of the encryption contents data in the data distribution system shown in drawing 1 and drawing 2 .

[Drawing 16] It is the 1st flow chart for explaining loan actuation of a license of the encryption contents data in the data distribution system shown in drawing 1 and drawing 2 .

[Drawing 17] It is the 2nd flow chart for explaining loan actuation of a license of the encryption contents data in the data distribution system shown in drawing 1 and drawing 2 .

[Drawing 18] It is the 1st flow chart for explaining return actuation of a license of the encryption contents data in the data distribution system shown in drawing 1 and drawing 2 .

[Drawing 19] It is the 2nd flow chart for explaining return actuation of a license of the encryption contents data in the data distribution system shown in drawing 1 and drawing 2 .

[Drawing 20] It is the 3rd flow chart for explaining return actuation of a license of the encryption contents data in the data distribution system shown in drawing 1 and drawing 2.

[Drawing 21] It is the 4th flow chart for explaining return actuation of a license of the encryption contents data in the data distribution system shown in drawing 1 and drawing 2.

[Drawing 22] It is drawing showing the configuration of the contents list file in the hard disk of a personal computer.

[Drawing 23] It is drawing showing the configuration of the playback list file in a memory card.

[Drawing 24] It is a flow chart for explaining the playback actuation in a playback terminal.

[Description of Notations]

10 Distribution Server, 20 Distribution Carrier, 30 Internet Network, 50 A personal computer, 60 Music CD, 70 USB cable, 100 A portable telephone, 102 A playback terminal, 110 Memory card, 130 A head telephone, 150 A contents list file, 160 Playback list file, 302 An accounting database, 304 An information database, 307 Menu database, 308 A distribution record database, 310 The data-processing section, 312, 320, 1404, 1408, 1412, 1422, 1504, 1510, 1516, 5204, 5208 and 5212, the 5222 decode processing section, 313 An authentication key attaching part, a 315 distribution control section, 316 Session key generating section, 318, 326, 328, 1406, 1410, 1417, 1506, 5206, 5210, 5217, 5405 Cipher-processing section, 350 A communication device, 510, 1106 and 1420, 5220 controllers, 520 A license management device and 530 550 A hard disk, 1112 USB interface, 555 A modem, 560 A keyboard, 570 Display, 580, 1114, 1426, 1530, 5226 terminals, 1108 Control panel, 1110 A display panel, 1200 Memory card interface, 1400, 1500, 5200 1402 The authentication data-hold section, 5202 Kmc attaching part, 1414 5214 1415 A KPa attaching part, 5215 Memory, 1415A A license field and 1415B 1416 A data area, 5216 KPmc attaching part, 1418 5218 1421 The session key generating section, 5221 Km attaching part, 1424 5224 An interface, 1442, 1446, 5242, 5246 Change-over switch, 1502 Kp1 attaching part, 1518 The music playback section, 1519 DA converter, 1521-1525, 1621-162n License management file, 1531-1535, 1611-161n Contents file, 1550 A contents regenerative circuit, 5400 A water mark detection means, 5401 A water mark judging means, 5402 A remark means, 5403 A license generating means, 5404 Music encoder.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-288448

(P2002-288448A)

(43) 公開日 平成14年10月4日 (2002. 10. 4)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)	
G 0 6 F 17/60	3 0 2	G 0 6 F 17/60	3 0 2 E	5 B 0 3 5
	Z E C		Z E C	5 B 0 5 8
	1 4 2		1 4 2	
	5 0 2		5 0 2	
G 0 6 K 17/00		G 0 6 K 17/00	L	
審査請求 未請求 請求項の数 9 O L (全 44 頁) 最終頁に続く				

(21) 出願番号 特願2001-87395(P2001-87395)

(22) 出願日 平成13年3月26日(2001. 3. 26)

(71) 出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72) 発明者 堀 吉宏

大阪府守口市京阪本通2丁目5番5号 三
洋電機株式会社内

(72) 発明者 吉川 隆敏

大阪府守口市京阪本通2丁目5番5号 三
洋電機株式会社内

(74) 代理人 100064746

弁理士 深見 久郎 (外3名)

Fターム(参考) 5B035 AA13 BB09 BC00 CA38

5B058 CA27 KA02 KA04 KA08 KA35

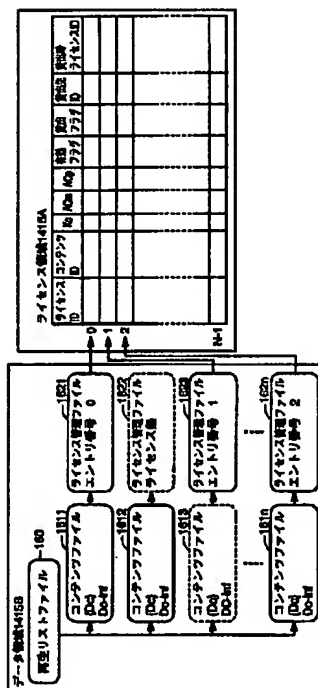
YA20

(54) 【発明の名称】 ライセンス記録装置

(57) 【要約】

【課題】 貸出したライセンスのバックアップを提供できるライセンス記録装置を提供する。

【解決手段】 メモリカードは、ライセンス領域1415Aを備える。ライセンス領域1415Aは、ライセンス(ライセンスID、コンテンツID、ライセンス鍵Kc、アクセス制御情報ACm、および再生回数制御情報ACp)、有効フラグ、貸出フラグ、貸出先ID、および貸出時ライセンスIDを含む。ライセンスの貸出が行なわれると、貸出フラグに「貸出中」が設定され、貸出先IDに貸出先のメモリカードに固有な公開暗号鍵が格納され、貸出時ライセンスIDに貸出用ライセンスIDが格納される。



【特許請求の範囲】

【請求項1】 暗号化コンテンツデータを復号するためのライセンスから貸出用ライセンスを生成し、前記貸出用ライセンスを他のライセンス記録装置へ貸出すライセンス記録装置であって、

前記ライセンスと、前記ライセンスの貸出可否を示す貸出フラグと、前記貸出用ライセンスの貸出先を特定するための貸出先特定情報と、前記貸出用ライセンスを識別するための貸出用ライセンス識別情報とを保持するライセンス保持部と、

制御部とを備え、

前記制御部は、前記ライセンスの貸出要求に応じて、前記他のライセンス記録装置への貸出の対象となるライセンスを指定するためのライセンス指定情報と前記貸出用ライセンスを特定するための貸出用ライセンス特定情報とを外部から受け、前記ライセンス指定情報によって指定されたライセンスを前記ライセンス保持部から読出し、その読出したライセンスに含まれ、かつ、前記読出したライセンスを特定するためのライセンス特定情報を前記貸出用ライセンス特定情報に代えて前記貸出用ライセンスを生成し、前記貸出フラグを貸出中に設定する、ライセンス記録装置。

【請求項2】 前記制御部は、前記ライセンス保持部から読出したライセンスが、複製を禁止され、かつ、移動が許可されたライセンスであるとき、前記貸出用ライセンスを生成する、請求項1に記載のライセンス記録装置。

【請求項3】 前記制御部は、前記貸出フラグが前記ライセンスを貸出していないことを示すとき、前記貸出用ライセンスを生成する、請求項1または請求項2に記載のライセンス記録装置。

【請求項4】 前記制御部は、さらに、前記他のライセンス記録装置における前記貸出用ライセンスの移動および複製を禁止するための制御情報を生成し、前記ライセンス保持部から読出したライセンスに含まれ、かつ、前記読出したライセンスの複製を禁止した制御情報を、前記生成した制御情報に代えて前記貸出用ライセンスを生成する、請求項1から請求項3のいずれか1項に記載のライセンス記録装置。

【請求項5】 前記制御部は、さらに、前記貸出用ライセンス特定情報を前記貸出用ライセンス識別情報として前記ライセンス保持部に格納する、請求項1から請求項4のいずれか1項に記載のライセンス記録装置。

【請求項6】 前記制御部は、さらに、前記他のライセンス記録装置に固有な公開暗号鍵を前記他のライセンス記録装置から受信し、その受信した公開暗号鍵を前記貸出先特定情報として前記ライセンス保持部に格納する、請求項1から請求項5のいずれか1項に記載のライセンス記録装置。

【請求項7】 前記ライセンス保持部は、領域を指定す

るエントリ番号に対応して前記ライセンス、前記貸出フラグ、前記貸出先特定情報、および前記貸出用ライセンス識別情報を格納しており、

前記制御部は、前記ライセンス指定情報として前記エントリ番号を外部から受ける、請求項1から請求項6のいずれか1項に記載のライセンス記録装置。

【請求項8】 前記ライセンス保持部は、前記貸出先特定情報と前記貸出用ライセンス識別情報とをライセンスの貸出先の数に応じて保持する、請求項1から請求項7のいずれか1項に記載のライセンス記録装置。

【請求項9】 前記ライセンスによって再生される暗号化コンテンツデータを記録するデータ格納部をさらに備える、請求項1から請求項8のいずれか1項に記載のライセンス記録装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムを用いて取得された暗号化データを復号および再生するためのライセンスを他のライセンス記録装置へ貸出すライセンス記録装置に関するものである。

【0002】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易に情報通信網にアクセスし、情報通信網上のデータを取得することが可能となっている。

【0003】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】したがって、このような情報通信網において音楽データや画像データ等の著作物の創作物であるコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】一方で、著作権保護の目的を最優先して、急拡大する情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】ここで、上述のような情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体

10

20

30

40

50

やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【0007】しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】このような事情からも、音楽データや画像データを情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0009】この場合、情報通信網を通じて公衆に送信される音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0010】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【0011】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【0012】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話に装着する。携帯電話は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【0013】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【0014】一方、インターネットを用いて暗号化コンテンツデータをパーソナルコンピュータに配信すること

も行なわれている。そして、パーソナルコンピュータへの暗号化コンテンツデータの配信においては、パーソナルコンピュータにインストールされたソフトウェアによって暗号化コンテンツデータの配信が行なわれており、暗号化コンテンツデータに対するセキュリティは、暗号化コンテンツデータをメモリカードに書き込む場合より低い。また、上記のメモリカードと同じセキュリティを持つデバイスをパーソナルコンピュータに装着すれば、上記の携帯電話機に対する暗号化コンテンツデータの配信と同じ配信をパーソナルコンピュータに対して行なうことが可能である。

【0015】そうすると、パーソナルコンピュータは、インストールされたソフトウェアと、上記デバイスとによって暗号化コンテンツデータを受信する。つまり、パーソナルコンピュータは、セキュリティレベルの異なる暗号化コンテンツデータを受信する。

【0016】さらに、音楽データが記録された音楽CDが広く普及しており、この音楽CDから音楽データをリッピングによって取得することも行なわれている。そして、このリッピングによって音楽データから暗号化音楽データ（暗号化コンテンツデータ）と、その暗号化音楽データを復号して再生するためのライセンスとが生成される。そして、このリッピングにおいては、コンテンツデータの利用規則を規定するウォーターマークをコンテンツデータから検出し、その検出したウォーターマークの内容に応じて暗号化コンテンツデータおよびライセンスが生成される。

【0017】上述したように、携帯電話機およびパーソナルコンピュータは、配信サーバから暗号化された暗号化コンテンツデータおよびライセンスを受信する。そして、携帯電話機およびパーソナルコンピュータのユーザは、受信した暗号化コンテンツデータおよびライセンスを他のユーザの携帯電話機またはパーソナルコンピュータへ移動または複製することもある。この場合、ユーザは、暗号化コンテンツデータを他のユーザの携帯電話機またはパーソナルコンピュータへ移動／複製することは自由であるが、暗号化コンテンツデータを復号するライセンスを他のユーザの携帯電話機またはパーソナルコンピュータへ自由に移動することはできない。つまり、ライセンスは、コンテンツ供給者の定めた条件に従って制御され、複製が自由に行なえるライセンス、複製を禁止するものの移動を許可するライセンス、複製・移動とともに禁止するライセンスが存在する。また、音楽CDからのリッピングでは、通常、著作権保護の観点から複製も移動も禁止しておく必要がある。他のユーザの携帯電話機またはパーソナルコンピュータへ移動したとき、暗号化コンテンツデータの著作権保護の観点から送信側と受信側との両方にライセンスを残すことはできない。そこで、ライセンスの移動を行なったとき、送信側のライセンスを消去する。

【0018】また、移動および複製が禁止されたライセンスに対しては、返却を条件として他のメモリカード等へライセンスを貸出すことが行なわれている。

【0019】

【発明が解決しようとする課題】しかし、従来のライセンスの貸出においては、貸出したライセンスと貸出元にあるライセンスとを1対1に対応付けて、貸出元において管理することができない。つまり、貸出元において、貸出したライセンスのバックアップを提供することができないという問題があった。

【0020】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、貸出したライセンスのバックアップを提供できるライセンス記録装置を提供することである。

【0021】

【課題を解決するための手段】この発明によれば、ライセンス記録装置は、暗号化コンテンツデータを復号するためのライセンスから貸出用ライセンスを生成し、貸出用ライセンスを他のライセンス記録装置へ貸出すライセンス記録装置であって、ライセンスと、ライセンスの貸出可否を示す貸出フラグと、貸出用ライセンスの貸出先を特定するための貸出先特定情報と、貸出用ライセンスを識別するための貸出用ライセンス識別情報とを保持するライセンス保持部と、制御部とを備え、制御部は、ライセンスの貸出要求に応じて、他のライセンス記録装置への貸出の対象となるライセンスを指定するためのライセンス指定情報と貸出用ライセンスを特定するための貸出用ライセンス特定情報とを外部から受け、ライセンス指定情報によって指定されたライセンスをライセンス保持部から読出し、その読出したライセンスに含まれ、かつ、読出したライセンスを特定するためのライセンス特定情報を貸出用ライセンス特定情報に代えて貸出用ライセンスを生成し、貸出フラグを貸出中に設定する。

【0022】好ましくは、制御部は、ライセンス保持部から読出したライセンスが、複製を禁止され、かつ、移動が許可されたライセンスであるとき、貸出用ライセンスを生成する。

【0023】好ましくは、制御部は、貸出フラグがライセンスを貸出していないことを示すとき、貸出用ライセンスを生成する。

【0024】好ましくは、制御部は、さらに、他のライセンス記録装置における貸出用ライセンスの移動および複製を禁止するための制御情報を生成し、ライセンス保持部から読出したライセンスに含まれ、かつ、読出したライセンスの複製を禁止した制御情報を、生成した制御情報に代えて貸出用ライセンスを生成する。

【0025】好ましくは、制御部は、さらに、貸出用ライセンス特定情報を貸出用ライセンス識別情報としてライセンス保持部に格納する。

【0026】好ましくは、制御部は、さらに、他のライ

センス記録装置に固有な公開暗号鍵を他のライセンス記録装置から受信し、その受信した公開暗号鍵を貸出先特定情報としてライセンス保持部に格納する。

【0027】好ましくは、ライセンス保持部は、領域を指定するエントリ番号に対応してライセンス、貸出フラグ、貸出先特定情報、および貸出用ライセンス識別情報を格納しており、制御部は、ライセンス指定情報としてエントリ番号を外部から受ける。

【0028】好ましくは、ライセンス保持部は、貸出先特定情報と貸出用ライセンス識別情報とをライセンスの貸出先の数に応じて保持する。

【0029】好ましくは、ライセンス記録装置は、ライセンスによって再生される暗号化コンテンツデータを記録するデータ格納部をさらに備える。

【0030】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0031】図1は、本発明によるライセンス記録装置が暗号化コンテンツデータを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0032】なお、以下では携帯電話網を介してデジタル音楽データをユーザの携帯電話に装着されたメモリカード110に、またはインターネットを介してデジタル音楽データを各パーソナルコンピュータに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画データ等を配信する場合においても適用することが可能なものである。

【0033】図1を参照して、配信キャリア20は、自己の携帯電話網を通じて得た、ユーザからの配信要求（配信リクエスト）を配信サーバ10に中継する。著作権の存在する音楽データを管理する配信サーバ10は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機100に装着されたメモリカード110が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア20である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報として暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスを与える。

【0034】配信キャリア20は、自己の携帯電話網を通じて配信要求を送信した携帯電話機100に装着されたメモリカード110に対して、携帯電話網および携帯電話機100を介して暗号化コンテンツデータとライセンスとを配信する。

【0035】図1においては、たとえば携帯電話ユーザの携帯電話機100には、着脱可能なメモリカード110が装着される構成となっている。メモリカード110は、携帯電話機100により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機100中の音楽再生部（図示せず）に与える。

【0036】さらに、たとえば携帯電話ユーザは、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【0037】このような構成とすることで、まず、メモリカード110を利用しないと、配信サーバ10からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【0038】しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0039】また、図1においては、パーソナルコンピュータ50は、メモリカード110のライセンス管理に関わる機能と同一機能を備えたライセンス管理デバイス（ハードウェア）を備えることで、携帯電話機100およびメモリカード110を用いて受信したのと同じセキュリティレベルの配信を受けることができる。そして、パーソナルコンピュータ50は、インターネット網30を介して、暗号化コンテンツデータとライセンスとを配信サーバ10から受信する。このとき、ライセンスは、配信サーバ10とライセンス管理デバイスとの間で所定の手順に従った暗号通信路を用いて、直接、ライセンス管理デバイスにおいて受信され、記録される。暗号化コンテンツデータはそのままHDDに記録される。このライセンス管理デバイスは、メモリカード110と同じようにライセンスの送受信や管理の機密性をハード的に保持するものであり、機密性が高いものである。

【0040】さらに、図1においては、パーソナルコンピュータ50は、ライセンス管理モジュールを使って音楽データを記録した音楽CD（Compact Disk）60から取得した音楽データからローカル使用に限定された暗号化コンテンツデータと、暗号化コンテンツデータを再生するためのライセンスとを生成する。この処理をリッピングと呼び、音楽CDから暗号化コンテンツデータとライセンスとを取得する行為に相当する。リッピングの詳細については後述する。

【0041】またさらに、パーソナルコンピュータ50は、USB（Universal Serial Bus）ケーブル70によって携帯電話機100と接続さ

れ、暗号化コンテンツデータおよびライセンスを携帯電話機100に装着されたメモリカード110と送受信することが可能である。

【0042】更に、図1においては、パーソナルコンピュータ50は、ハードウェアによって機密性を持つコンテンツ再生回路をパーソナルコンピュータに備えれば暗号化コンテンツデータの再生が可能となる。また、ソフトウェアによるコンテンツ再生であっても、十分な機密性が確保できれば、再生可能となる。パーソナルコンピュータにおける再生についての詳細な説明は、本出願における説明を簡略化するために省略する。

【0043】したがって、図1に示すデータ配信システムにおいては、パーソナルコンピュータ50は、インターネット網30を介して配信サーバ10から暗号化コンテンツデータとライセンスとを受信するとともに、音楽CDから暗号化コンテンツデータとライセンスとを取得する。また、携帯電話機100に装着されたメモリカード110は、携帯電話網を介して配信サーバ10から暗号化コンテンツデータおよびライセンスを受信するとともに、パーソナルコンピュータ50が配信サーバ10または音楽CD60から取得した暗号化コンテンツデータおよびライセンスを受信する。携帯電話機100のユーザは、パーソナルコンピュータ50を介することによって音楽CDから暗号化コンテンツデータおよびライセンスを取得することが可能となる。

【0044】さらに、携帯電話機100に装着されたメモリカード110は、携帯電話網を介して配信サーバ10から受信した暗号化コンテンツデータおよびライセンスをパーソナルコンピュータ50に待避することが可能となる。

【0045】図2は、携帯電話網を介して配信サーバ10から暗号化コンテンツデータおよびライセンスを受信する機能を有しない再生端末102を用いた場合のデータ配信システムを示したものである。図2に示すデータ配信システムにおいては、再生端末102に装着されたメモリカード110は、パーソナルコンピュータ50が配信サーバ10または音楽CD60から取得した暗号化コンテンツデータおよびライセンスを受信する。このように、パーソナルコンピュータ50が暗号化コンテンツデータおよびライセンスを取得することによって通信機能のない再生端末102のユーザも暗号化コンテンツデータを受信することができるようになる。

【0046】図1および図2に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話またはパーソナルコンピュータのユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号鍵を配信するための方式であり、さらに第2には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第3には、このように配信されたコンテンツデータの無断コピーを防止するため

のコンテンツデータ保護を実現する構成である。

【0047】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生できるデータ再生端末を携帯電話機またはパーソナルコンピュータとも言う。以下同じ）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【0048】なお、以下の説明においては、配信サーバ10から、各携帯電話機、各パーソナルコンピュータ等にコンテンツデータを伝送する処理を「配信」と称することとする。

【0049】図3は、図1および図2に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【0050】まず、配信サーバ10より配信されるデータについて説明する。Dcは、音楽データ等のコンテンツデータである。コンテンツデータDcは、ライセンス鍵Kcで復号可能な暗号化が施される。ライセンス鍵Kcによって復号可能な暗号化が施された暗号化コンテンツデータ{Dc}Kcがこの形式で配信サーバ10より携帯電話またはパーソナルコンピュータのユーザに配布される。

【0051】なお、以下においては、{Y}Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0052】さらに、配信サーバ10からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Dc-infが配布される。また、ライセンスとして、ライセンス鍵Kc、配信サーバ10からのライセンス鍵等を特定するための管理コードであるライセンスIDが配信サーバ10と携帯電話機100との間、または配信サーバ10とパーソナルコンピュータ50との間でやり取りされる。また、配信によらないライセンス、すなわち、ローカルでの使用を目的とするライセンスを特定するためにもライセンスIDは使用される。配信によるものと、ローカル使用のものとを区別するために、ライセンスIDの先頭は“0”で始まるものがローカル使用のライセンスIDであり、“0”以外から始まるものを配信によるライセンスIDであるとする。さらに、ライセンスとしては、コンテンツデータDcを識別するためのコードであるコンテンツIDや、コンテンツ供給者側の意向や利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、記録装置（メモリカード、またはライセンス管理デバイス）におけるライセンスのアクセスに対する制限に関する情報であるア

クセス制御情報ACmおよびデータ再生端末における再生に関する制御情報である再生制御情報ACp等が存在する。具体的には、アクセス制御情報ACmはメモリカード、およびライセンス管理デバイスからのライセンスまたはライセンス鍵を外部に出力するに当たっての制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する数）、ライセンスの移動・複製に関する制限情報およびライセンスのセキュリティレベルなどがある。再生制御情報ACpは、再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【0053】以後、コンテンツIDとライセンス鍵KcとライセンスIDとアクセス制御情報ACmと再生制御情報ACpとを併せて、ライセンスと総称することとする。

【0054】また、以降では、簡単化のためアクセス制御情報ACmは再生回数の制限を行なう制御情報である再生回数（0：再生不可、1～254：再生可能回数、255：制限無し）、ライセンスの移動および複製を制限する移動・複製フラグ（1：移動複製可、2：移動のみ可、3：移動複製禁止）の2項目とし、再生制御情報ACpは再生可能な期限を規定する制御情報である再生期限（UTCtimeコード）のみを制限するものとする。

【0055】本発明の実施の形態においては、送信元の記録装置（メモリカード、またはライセンス管理デバイス）から受信先の記録装置へのライセンスの移動／複製において、送信元の記録装置に保持されたライセンスの有効・無効を示す有効フラグの運用を行なう。この有効フラグが有効であるとき、ライセンスをメモリカードから外部へ出すことが可能であることを意味し、有効フラグが無効であるとき、ライセンスをメモリカードから外部へ出すことができないことを意味する。

【0056】また、送信元の記録装置から受信先の記録装置へのライセンスの貸出／返却において、送信元の記録装置に保持されたライセンスが他の記録装置へ貸出が可能か否かを示す貸出フラグ、ライセンスの貸出先を特定するための情報である貸出先ID、および貸出したライセンスを識別するための識別情報である貸出時ライセンスIDの運用を行なう。

【0057】図4は、図1および図2に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【0058】コンテンツ再生回路には固有の公開暗号鍵Kppyが設けられ、メモリカード、およびライセンス管理デバイスには固有の公開暗号鍵Kpmwが設けられる。そして、公開暗号鍵KppyおよびKpmwは、コンテンツ再生回路に固有の秘密復号鍵Kpyおよびメモリカード、ライセンス管理デバイスに固有の秘密復号鍵

Kmwによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、コンテンツ再生回路、メモリカード、およびライセンス管理デバイスの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【0059】また、コンテンツ再生回路（携帯電話機、再生端末）のクラス証明書としてCpyが設けられ、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書としてCmwが設けられる。これらのクラス証明書は、コンテンツ再生回路、メモリカード、およびライセンス管理デバイスのクラスごとに異なる情報を有する。耐タンパモジュールが破られたり、クラス鍵による暗号が破られた、すなわち、秘密復号鍵が漏洩したクラスは、ライセンス取得の禁止対象となる。

【0060】これらのコンテンツ再生回路のクラス公開暗号鍵およびクラス証明書は、認証データ {K Ppy / Cpy} KPaの形式で、メモリカード、およびライセンス管理デバイスのクラス公開暗号鍵およびクラス証明書は認証データ {K Pmw / Cmw} KPaの形式で出荷時にデータ再生回路、メモリカード、およびライセンス管理デバイスにそれぞれ記録される。後ほど詳細に説明するが、KPaは、配信システム全体で共通の公開認証鍵である。

【0061】また、メモリカード110、およびライセンス管理デバイスのデータ処理を管理するための鍵として、メモリカード、およびライセンス管理デバイスという媒体ごとに設定される公開暗号鍵K Pmcxと、公開暗号鍵K Pmcxで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵Kmcxが存在する。このメモリカードごとに個別な公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵K Pmcxを個別公開暗号鍵、秘密復号鍵Kmcxを個別秘密復号鍵と称する。

【0062】メモリカードとの、またはライセンス管理デバイスに対するデータ授受における秘密保持のための暗号鍵として、ライセンスの配信、および再生が行なわれるごとに配信サーバ10、携帯電話機100、メモリカード110、ライセンス管理デバイスにおいて生成される共通鍵Ks1~Ks3が用いられる。

【0063】ここで、共通鍵Ks1~Ks3は、配信サーバ、コンテンツ再生回路もしくはメモリカードもしくはライセンス管理デバイスもしくはライセンス管理モジュール間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ks1~Ks3を「セッションキー」とも呼ぶこととする。

【0064】これらのセッションキーKs1~Ks3は、各セッションごとに固有の値を有することにより、配信サーバ、コンテンツ再生回路、メモリカード、およびライセンス管理デバイスによって管理される。具体的には、セッションキーKs1は、配信サーバによって配信セッションごとに発生される。セッションキーKs2は、メモリカード、およびライセンス管理デバイスによって全てのセッションにおいてセッションごとに発生し、セッションキーKs3は、コンテンツ再生回路において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行した上でライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0065】図5は、図1および図2に示した配信サーバ10の構成を示す概略ブロック図である。

【0066】配信サーバ10は、コンテンツデータを所定の方式に従って暗号化したデータやコンテンツID等の配信情報を保持するための情報データベース304と、携帯電話やパーソナルコンピュータの各ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース302と、情報データベース304に保持されたコンテンツデータのメニューを保持するメニューデータベース307と、ライセンスの配信ごとにコンテンツデータおよびライセンス鍵等の配信を特定するトランザクションID等の配信に関するログを保持する配信記録データベース308と、情報データベース304、課金データベース302、メニューデータベース307、および配信記録データベース308からのデータをバスBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【0067】データ処理部310は、バスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315に制御されて、配信セッション時にセッションキーKs1を発生するためのセッションキー発生部316と、メモリカード、およびライセンス管理デバイスから送られてきた認証のための認証データ {K Pmw / Cmw} KPaを復号するための2種類の公開認証鍵KPaを保持する認証鍵保持部313と、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールから送られてきた認証のための認証データ {K Pmw / Cmw} KPaを通信装置350およびバスBS1を介して受けて、認証鍵保持部313からの公開認証鍵KPaまたはK Pbによって復号処理を行なう復号処理部312と、配信セッションごとに、セッション鍵Ks1を発生するセッションキー発生部316、セッションキー発生部3

16より生成されたセッションキーKs1を復号処理部312によって得られたクラス公開暗号鍵Kpmwを用いて暗号化して、バスBS1に出力するための暗号化処理部318と、セッションキーKs1によって暗号化された上で送信されたデータをバスBS1より受けて、復号処理を行なう復号処理部320を含む。

【0068】データ処理部310は、さらに、配信制御部315から与えられるライセンス鍵Kcおよびアクセス制御情報ACmを、復号処理部320によって得られたメモリカード、およびライセンス管理デバイスの個別公開暗号鍵Kpmcxによって暗号化するための暗号化処理部326と、暗号化処理部326の出力を、復号処理部320から与えられるセッションキーKs2によってさらに暗号化してバスBS1に出力するための暗号化処理部328を含む。

【0069】配信サーバ10の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0070】図6は、図1および図2に示したパーソナルコンピュータ50の構成を説明するための概略ブロック図である。パーソナルコンピュータ50は、パーソナルコンピュータ50の各部のデータ授受を行なうためのバスBS2と、パーソナルコンピュータ内を制御すると共に、各種のプログラムを実行するためのコントローラ(CPU)510と、データバスBS2と、データバスBS2に接続され、プログラムやデータを記録し、蓄積しておくための大容量記録装置であるハードディスク(HDD)530およびCD-ROMドライブ540と、ユーザからの指示を入力するためのキーボード560と、各種の情報を視覚的にユーザに与えるためのディスプレイ570を含む。

【0071】パーソナルコンピュータ50は、さらに、暗号化コンテンツデータおよびライセンスを携帯電話機100等へ通信する際にコントローラ510と端子580との間でデータの授受を制御するためのUSBインタフェース550と、USBケーブル70を接続するための端子580と、配信サーバ10とインターネット網30を介して通信する際にコントローラ510と端子585との間でデータの授受を制御するためのモデム555と、インターネット網30と接続するための端子585を含む。

【0072】コントローラ510は、プログラムであるライセンス管理モジュール511を実行することでインターネット網30を介して暗号化コンテンツデータおよびライセンスを配信サーバ10から取得するために、配信サーバ10との間でデータの授受を制御するとともに、CD-ROMドライブ540を介して音楽CDからリッピングによって暗号化コンテンツデータおよびライセンスを取得する際の制御を行なう。さらに、パーソナルコンピュータ50は、配信サーバ10からのライセン

スの受信を行なう際に配信サーバ10との間で、またはライセンス管理モジュール511からリッピングによるライセンスの受信を行なう際にはライセンス管理モジュール511との間で各種の鍵のやり取りを行ない、配信された暗号化コンテンツデータを再生するためのライセンスをハード的に管理するライセンス管理デバイス520を含む。

【0073】図7は、図2に示した再生端末102の構成を説明するための概略ブロック図である。

【0074】再生端末102は、再生端末102の各部のデータ授受を行なうためのバスBS3と、バスBS3を介して再生端末102の動作を制御するためのコントローラ1106と、外部からの指示を再生端末102に与えるための操作パネル1108と、コントローラ1106等から出力される情報をユーザに視覚情報として与えるための表示パネル1110を含む。

【0075】再生端末102は、さらに、配信サーバ10からのコンテンツデータ(音楽データ)を記憶し、かつ、復号処理を行なうための着脱可能なメモリカード110と、メモリカード110とバスBS3との間のデータの授受を制御するためのメモリカードインタフェース1200と、パーソナルコンピュータ50から暗号化コンテンツデータおよびライセンスを受信する際にバスBS3と端子1114との間のデータ授受を制御するためのUSBインタフェース1112と、USBケーブル70を接続するための端子1114を含む。

【0076】再生端末102は、さらに、クラス公開暗号鍵Kpp1およびクラス証明書Cp1を公開認証鍵KPaで復号することでその正当性を認証できる状態に暗号化した認証データ{Kpp1/Cp1}KPaを保持する認証データ保持部1500を含む。ここで、再生端末102のクラスyは、y=1であるとする。

【0077】再生端末102は、さらに、クラス固有の復号鍵であるKp1を保持するKp1保持部1502と、バスBS3から受けたデータをKp1によって復号し、メモリカード110によって発生されたセッションキーKs2を得る復号処理部1504を含む。

【0078】再生端末102は、さらに、メモリカード110に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110との間でバスBS3上においてやり取りされるデータを暗号化するためのセッションキーKs3を乱数等により発生するセッションキー発生部1508と、暗号化コンテンツデータの再生セッションにおいてメモリカード110からライセンス鍵Kcおよび再生制御情報ACpを受取る際に、セッションキー発生部1508により発生されたセッションキーKs3を復号処理部1504によって得られたセッションキーKs2によって暗号化し、バスBS3に出力する暗号化処理部1506を含む。

【0079】再生端末102は、さらに、バスBS3上

のデータをセッションキーKs3によって復号して、ライセンス鍵Kcおよび再生制御情報ACpを出力する復号処理部1510と、バスBS3より暗号化コンテンツデータ{Dc}Kcを受けて、復号処理部1510によって復号されたライセンス鍵Kcによって暗号化コンテンツデータ{Dc}Kcを復号する復号処理部1516とを含む。

【0080】再生端末102は、さらに、復号処理部1516からの出力を受けてコンテンツデータを再生するための音楽再生部1518と、音楽再生部1518の出力をデジタル信号からアナログ信号に変換するDA変換器1519と、DA変換器1519の出力をヘッドホンなどの外部出力装置（図示省略）へ出力するための端子1530とを含む。

【0081】なお、図7においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生回路1550を構成する。

【0082】一方、図1に示す携帯電話機100は、携帯電話網を介して配信サーバ10から暗号化コンテンツデータあるいはライセンスの配信を受信する機能を有するものである。したがって、図1に示す携帯電話機100の構成は、図7に示す構成において、携帯電話網により無線伝送される信号を受信するためのアンテナと、アンテナからの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナに与えるための送受信部とマイクとスピーカと音声コーデック等の携帯電話機が本来備える機能を設けたものである。

【0083】携帯電話機100、再生端末102の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0084】図8は、図1および図2に示すメモリカード110の構成を説明するための概略ブロック図である。

【0085】既に説明したように、メモリカードのクラス公開暗号鍵およびクラス秘密復号鍵として、KpmwおよびKmwが設けられ、メモリカードのクラス証明書Cmwが設けられるが、メモリカード110においては、自然数w=3で表わされるものとする。また、メモリカードを識別する自然数xはx=4で表されるものとする。

【0086】したがって、メモリカード110は、認証データ{Kpm3/Cm3}Kpaを保持する認証データ保持部1400と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵Kmc4を保持するKmc保持部1402と、クラス秘密復号鍵Km3を保持するKm保持部1421と、個別秘密復号鍵Kmc4によって復号可能な公開暗号鍵Kpmc4を保持するKpmc保持部1416とを含む。

【0087】このように、メモリカードという記録装置

の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【0088】メモリカード110は、さらに、メモリカードインタフェース1200との間で信号を端子1426を介して授受するインタフェース1424と、インタフェース1424との間で信号をやり取りするバスBS4と、バスBS4にインタフェース1424から与えられるデータから、クラス秘密復号鍵Km3をKm保持部1421から受けて、配信サーバ10が配信セッションにおいて生成したセッションキーKs1を接点Paに出力する復号処理部1422と、Kpa保持部1414から公開認証鍵Kpaを受けて、バスBS4に与えられるデータから公開認証鍵Kpaによる復号処理を実行して復号結果と得られたクラス証明書をコントローラ1420に、得られたクラス公開鍵を暗号化処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1446によって選択的に与えられるデータを暗号化してバスBS4に出力する暗号化処理部1406とを含む。

【0089】メモリカード110は、さらに、配信、および再生の各セッションにおいてセッションキーKs2を発生するセッションキー発生部1418と、セッションキー発生部1418の出力したセッションキーKs2を復号処理部1408によって得られるクラス公開暗号鍵KppyもしくはKpmwによって暗号化してバスBS4に送出する暗号化処理部1410と、バスBS4よりセッションキーKs2によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキーKs2によって復号する復号処理部1412と、暗号化コンテンツデータの再生セッションにおいてメモリ1415から読出されたライセンス鍵Kcおよび再生制御情報ACpを、復号処理部1412で復号された他のメモリカード110の個別公開暗号鍵Kpmcx(≠4)で暗号化する暗号処理部1417とを含む。

【0090】メモリカード110は、さらに、バスBS4上のデータを個別公開暗号鍵Kpmc4と対をなすメモリカード110の個別秘密復号鍵Kmc4によって復号するための復号処理部1404と、暗号化コンテンツデータ{Dc}Kcと、暗号化コンテンツデータ{Dc}Kcを再生するためのライセンス(Kc, ACp, ACm, ライセンスID, コンテンツID)と、有効フラグと、貸出先IDと、貸出時ライセンスIDと、付加情報Dc-infと、メモリカード110内に格納される暗号化コンテンツデータを管理する再生リストファイルと、ライセンスを管理するためのライセンス管理ファイルとをバスBS4より受けて格納するためのメモリ1415とを含む。メモリ1415は、例えば半導体メモ

りによって構成される。また、メモリ1415は、ライセンス領域1415Aと、データ領域1415Bとから成る。ライセンス領域1415Aは、ライセンス、有効フラグ、貸出先ID、および貸出時ライセンスIDを記録するための領域である。データ領域1415Bは、暗号化コンテンツデータ {Dc} Kc、暗号化コンテンツデータの関連情報Dc-inf、ライセンスを管理するために必要な情報を暗号化コンテンツごとに記録するライセンス管理ファイル、およびメモリカードに記録された暗号化コンテンツデータやライセンスにアクセスするための基本的な情報を記録する再生リストファイルを記録するための領域である。そして、データ領域1415Bは、外部から直接アクセスが可能である。ライセンス管理ファイルおよび再生リストファイルの詳細については後述する。

【0091】ライセンス領域1415Aは、ライセンス（ライセンス鍵Kc、再生制御情報ACp、アクセス制限情報ACm、ライセンスID、コンテンツID）、有効フラグ、貸出先ID、および貸出時ライセンスIDを記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンス、有効フラグ、貸出先ID、および貸出時ライセンスIDを格納する。ライセンス等に対してアクセスする場合には、ライセンス等が格納されている、あるいは、ライセンス等を記録したいエントリをエントリ番号によって指定する構成になっている。

【0092】メモリカード110は、さらに、バスBS4を介して外部との間でデータ授受を行ない、バスBS4との間で再生情報等を受けて、メモリカード110の動作を制御するためのコントローラ1420を含む。

【0093】なお、ライセンス領域1415Aは、耐タンパモジュール領域に構成される。また、ライセンス領域1415Aとデータ領域1415Bとは、1つのメモリ1415内に構成されている必要はなく、それぞれ、別々に構成されていても良い。さらに、メモリ1415は、データ領域1415Bを伴わないライセンス専用の領域であってもよい。

【0094】図9は、パーソナルコンピュータ50に内蔵されたライセンス管理デバイス520の構成を示す概略ブロック図である。ライセンス管理デバイス520は、メモリカード110におけるデータ領域1415Bに相当する領域を必要としない点、インタフェース1424の機能および端子1426の形状が異なるインタフェース5224と端子5226とを備える点が異なるのみで、基本的にメモリカード110と同じ構成から成る。ライセンス管理デバイス520の認証データ保持部5200、Kmc保持部5202、復号処理部5204、暗号処理部5206、復号処理部5208、暗号処理部5210、復号処理部5212、KPa保持部5214、KPMC保持部5216、暗号処理部5217、セッションキー発生部5218、コントローラ5220、Km

保持部5221、復号処理部5222、インタフェース5224、端子5226、切換スイッチ5242、5246は、それぞれ、メモリカード110の認証データ保持部1400、Kmc保持部1402、復号処理部1404、暗号処理部1406、復号処理部1408、暗号処理部1410、復号処理部1412、KPa保持部1414、KPMC保持部1416、暗号処理部1417、セッションキー発生部1418、コントローラ1420、Km保持部1421、復号処理部1422、切換スイッチ1442、1446と同じである。ただし、認証データ保持部5200は、認証データ {KPM7/Cm7} KPaを保持し、KPMC保持部5216は、個別公開暗号鍵KPM8を保持し、Km保持部5202は、クラス秘密復号鍵Km7を保持し、Kmc保持部5221は、個別秘密復号鍵Kmc8を保持する。ライセンス管理デバイス520のクラスを表す自然数wはw=7であり、ライセンス管理デバイス520を識別するための自然数xはx=8であるとする。

【0095】ライセンス管理デバイス520は、ライセンス (Kc, ACp, ACm, ライセンスID, コンテンツID) と、有効フラグと、貸出先IDと、貸出時ライセンスIDとを記録するメモリ5215を、メモリカード110のメモリ1415に代えて含む。メモリ5215は、ライセンス、有効フラグ、貸出先ID、および貸出時ライセンスIDを記録したライセンス領域5215Aを含む。

【0096】以下、図1および図2に示すデータ配信システムにおける各セッションの動作について説明する。

【0097】【配信】図10および図11は、図1および図2に示すデータ配信システムのパーソナルコンピュータ50における暗号化コンテンツデータおよびライセンスの購入時に発生する配信セッションを説明するための第1および第2のフローチャートである。なお、この動作を「配信」と言う。

【0098】図10における処理以前に、パーソナルコンピュータ50のユーザは、配信サーバ10に対してインターネット網30を介して接続し、購入を希望するコンテンツに対するコンテンツIDを取得していることを前提としている。

【0099】図10を参照して、パーソナルコンピュータ50のユーザからキーボード560を介してコンテンツIDの指定による配信リクエストがなされる（ステップS100）。そして、キーボード560を介して暗号化コンテンツデータのライセンスを購入するための購入条件ACが入力される（ステップS102）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Kcを購入するために、暗号化コンテンツデータのアクセス制御情報ACm、および再生制御情報ACpを想定して購入条件ACが入力される。

【0100】暗号化コンテンツデータの購入条件ACが

10

20

30

40

50

入力されると、コントローラ510は、バスBS2を介してライセンス管理デバイス520へ認証データの出力指示を与える(ステップS104)。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224およびバスBS5を介して認証データの送信要求を受信する(ステップS106)。そして、コントローラ5220は、バスBS5を介して認証データ保持部5200から認証データ{K P m7//Cm7} K P aを読み出し、{K P m7//Cm7} K P aをバスBS5、インタフェース5224および端子5226を介して出力する(ステップS108)。

【0101】パーソナルコンピュータ50のコントローラ510は、ライセンス管理デバイス520からの認証データ{K P m3//Cm3} K P aに加えて、コンテンツID、ライセンス購入条件のデータAC、および配信リクエストをモデム555およびインターネット網30を介して配信サーバ10に対して送信する(ステップS110)。

【0102】配信サーバ10では、パーソナルコンピュータ50から配信リクエスト、コンテンツID、認証データ{K P m7//Cm7} K P a、およびライセンス購入条件のデータACを受信し(ステップS112)、復号処理部312においてライセンス管理デバイス520から出力された認証データを公開認証鍵K P aで復号処理を実行する(ステップS114)。

【0103】配信制御部315は、復号処理部312における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS116)。正当な認証データであると判断された場合、配信制御部315は、クラス公開暗号鍵K P m7およびクラス証明書Cm7を承認し、受理する。そして、次の処理(ステップS118)へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵K P m7およびクラス証明書Cm7を受理しないで配信セッションを終了する(ステップS166)。

【0104】認証の結果、正当な認証データを持つライセンス管理デバイスを装着したパーソナルコンピュータからのアクセスであることが確認されると、配信サーバ10において、セッションキー発生部316は、配信のためのセッションキーK s1を生成する(ステップS118)。セッションキーK s1は、復号処理部312によって得られたメモリカード110に対応するクラス公開暗号鍵K P m7によって、暗号化処理部318によって暗号化される(ステップS120)。

【0105】配信制御部315は、ライセンスIDを生成し(ステップS122)、ライセンスIDおよび暗号化されたセッションキーK s1は、ライセンスID//{K s1} K m3として、バスBS1および通信装置3

50を介して外部に出力される(ステップS124)。

【0106】パーソナルコンピュータ50が、ライセンスID//{K s1} K m7を受信すると、コントローラ510は、ライセンスID//{K s1} K m7をメモリカード110に入力する(ステップS126)。そうすると、ライセンス管理デバイス520においては、端子5226およびインタフェース5224を介して、コントローラ5220は、ライセンスID//{K s1} K m7を受信する(ステップS128)。そして、コントローラ5220は、バスBS5を介して{K s1} K m7を復号処理部5222へ与え、復号処理部5222は、K m保持部5221に保持されるライセンス管理デバイス520に固有なクラス秘密復号鍵K m3によって復号処理することにより、セッションキーK s1を復号し、セッションキーK s1を受信する(ステップS130)。

【0107】コントローラ5220は、配信サーバ10で生成されたセッションキーK s1の受理を確認すると、セッションキー発生部5218に対してライセンス管理デバイス520において配信動作時に生成されるセッションキーK s2の生成を指示する。そして、セッションキー発生部5218は、セッションキーK s2を生成する(ステップS132)。

【0108】暗号化処理部5206は、切換スイッチ5242の接点P aを介して復号処理部5222より与えられるセッションキーK s1によって、切換スイッチ5246の接点を順次切換えることによって与えられるセッションキーK s2、および個別公開暗号鍵K P m c8を1つのデータ列として暗号化して、{K s2//K P m c8} K s1をバスBS5に出力する。バスBS5に出力された暗号化データ{K s2//K P m c8} K s1は、バスBS5からインタフェース5224および端子5226を介してパーソナルコンピュータ50に出力され(ステップS134)、パーソナルコンピュータ50から配信サーバ10に送信される(ステップS136)。

【0109】図11を参照して、配信サーバ10は、{K s2//K P m c8} K s1を受信して、復号処理部320においてセッションキーK s1による復号処理を実行し、ライセンス管理デバイス520で生成されたセッションキーK s2、およびライセンス管理デバイス520に固有の公開暗号鍵K P m c8を受信する(ステップS138)。

【0110】配信制御部315は、ステップS112で取得したコンテンツIDに従ってライセンス鍵K cを情報データベース304から取得し(ステップS140)、ステップS112で取得したライセンス購入条件のデータACに従って、アクセス制御情報A C mおよび再生制御情報A C pを決定する(ステップS142)。

【0111】配信制御部315は、生成したライセン

ス、すなわち、ライセンスID、コンテンツID、ライセンス鍵Kc、再生制御情報ACp、およびアクセス制御情報ACmを暗号化処理部326に与える。暗号化処理部326は、復号処理部320によって得られたライセンス管理デバイス520に固有の公開暗号鍵Kpmc8によってライセンスを暗号化して暗号化データ {ライセンスID//コンテンツID//Kc//ACm//ACp} Kmc8を生成する(ステップS144)。そして、暗号化処理部328は、暗号化処理部326からの暗号化データ {ライセンスID//コンテンツID//Kc//ACm//ACp} Kmc8を、復号処理部320からのセッションキーKs2によって暗号化し、暗号化データ { {ライセンスID//コンテンツID//Kc//ACm//ACp} Kmc8} Ks2を出力する。配信制御部315は、バスBS1および通信装置350を介して暗号化データ { {ライセンスID//コンテンツID//Kc//ACm//ACp} Kmc8} Ks2をパーソナルコンピュータ50へ送信する(ステップS146)。

【0112】パーソナルコンピュータ50は、送信された暗号化データ { {ライセンスID//コンテンツID//Kc//ACm//ACp} Kmc8} Ks2を受信し、バスBS2を介してライセンス管理デバイス520に入力する(ステップS148)。ライセンス管理デバイス520においては、端子5226およびインタフェース5224を介して、バスBS5に与えられた受信データを復号処理部5212によって復号する。復号処理部5212は、セッションキー発生部5218から与えられたセッションキーKs2を用いてバスBS5の受信データを復号し、バスBS5に出力する(ステップS150)。

【0113】この段階で、バスBS5には、Kmc保持部5202に保持される秘密復号鍵Kmc8で復号可能な暗号化ライセンス {ライセンスID//コンテンツID//Kc//ACm//ACp} Kmc8が出力される(ステップS150)。

【0114】コントローラ5220の指示によって、暗号化ライセンス {ライセンスID//コンテンツID//Kc//ACm//ACp} Kmc8は、復号処理部5204において、個別秘密復号鍵Kmc8によって復号され、ライセンス(ライセンス鍵Kc、ライセンスID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp)が受理される(ステップS152)。

【0115】パーソナルコンピュータ50のコントローラ510は、HDD530から読出したライセンス管理ファイルに基づいて、配信サーバ10から受信したライセンスを格納するためのエントリ番号を決定し、その決定したエントリ番号をバスBS2を介してライセンス管理デバイス520へ入力する。そして、コントローラ5

10は、ライセンス管理ファイルのライセンス管理情報を追加更新する(ステップS154)。

【0116】そうすると、ライセンス管理デバイス520のコントローラ5220は、ステップS152において取得したアクセス制御情報ACmに基づいて、取得したライセンスが貸出可能か否かを判定する(ステップS156)。アクセス制御情報ACmは、複製・移動制御情報と再生回数制御情報とから成る。複製・移動制御情報として「1」、「2」、および「3」のいずれかが設定されており、「1」はライセンスの複製・移動不可を意味し、「2」は複製不可・移動可を意味し、「3」は複製・移動禁止を意味する。また、再生回数制御情報としては、0~255の値が設定されている。そして、0~254の値は、設定された値の回数だけ暗号化コンテンツデータの再生が可能であることを意味し、255は、暗号化コンテンツデータを無制限に再生できることを意味する。本発明においては、複製・移動制御情報が「2」に設定され、かつ、再生回数制御情報が「255」に設定されているとき、ライセンスを貸出できるものとする。なお、再生回数制御情報が「255」に設定されていることは、ライセンスの貸出を可能にするための必須条件である。再生回数制御情報が「0~254」に設定されているときは、再生回数に制限があり、貸出元と貸出先とで何回、暗号化コンテンツデータを再生したかを管理するのは困難であるため再生回数が有限のときはライセンスの貸出を禁止し、再生回数が無限の場合に限りライセンスの貸出を可能にしたものである。

【0117】そして、コントローラ5220は、ライセンスの貸出が可能であれば、メモリ5215のライセンス領域5215Aのエントリ番号によって指定された領域に格納された貸出フラグを「可」に設定する(ステップS158)。一方、ステップS156において、ライセンスの貸出が不可と判定されたとき、コントローラ5220は、ライセンス領域5215Aのエントリ番号によって指定された領域に格納された貸出フラグを「不可」に設定する(ステップS160)。

【0118】ステップS158またはステップS160の後、コントローラ5220は、ライセンス領域5215Aのエントリ番号によって指定された領域に格納された有効フラグを「有効」に設定し(ステップS162)、ライセンス領域5215Aのエントリ番号によって指定された領域に、ステップS152において受理したライセンス(ライセンスID、コンテンツID、ライセンス鍵Kc、アクセス制御情報ACm、および再生制御情報ACp)を格納する(ステップS164)。そして、ライセンスの配信動作は終了する(ステップS166)。

【0119】ライセンスの配信動作が終了した後、パーソナルコンピュータ50のコントローラ510は、暗号化コンテンツデータの配信要求を配信サーバ10へ送信

し、配信サーバ10は、暗号化コンテンツデータの配信要求を受信する。そして、配信サーバ10の配信制御部315は、情報データベース304より、暗号化コンテンツデータ {Dc} Kcおよび付加情報Dc-infを取得して、これらのデータをバスBS1および通信装置350を介して出力する。

【0120】パーソナルコンピュータ50は、{Dc} Kc/Dc-infを受信して、暗号化コンテンツデータ {Dc} Kcおよび付加情報Dc-infを受信する。そうすると、コントローラ1106は、暗号化コンテンツデータ {Dc} Kcおよび付加情報Dc-infを1つのコンテンツファイルとしてバスBS2を介してHDD530に入力する。また、コントローラ510は、ライセンス管理デバイス520に格納されたライセンスのエントリ番号と、平文のライセンスIDおよびコンテンツIDを含む暗号化コンテンツデータ {Dc} Kcと付加情報Dc-infに対するライセンス管理ファイルを生成し、バスBS2を介してHDD530に入力する。さらに、コントローラ510は、HDD530に記録されているコンテンツリストファイルに受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や、付加情報Dc-infから抽出した暗号化コンテンツデータに関する情報(曲名、アーティスト名)等を追記し、全体の処理が終了する。

【0121】このようにして、パーソナルコンピュータ50に内蔵されたライセンス管理デバイス520が正規の認証データを保持する機器であること、同時に、クラス証明書Cm7とともに暗号化して送信できた公開暗号鍵Kpm7が有効であることを確認した上でライセンスを配信することができ、不正なライセンス管理デバイスへのライセンスの配信を禁止することができる。

【0122】さらに、配信サーバおよびライセンスかんりデバイス520でそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【0123】図1に示すデータ配信システムにおいて携帯電話機100に装着されたメモリカード110に対して、直接、ライセンスを配信する動作も図10および図11に示すフローチャートに従って行なわれる。すなわち、上記の説明において、パーソナルコンピュータ50を携帯電話機100に代え、ライセンス管理デバイス520をメモリカード110に代えれば良い。また、図10のステップS108においては、認証データ {Kpm7/Cm7} Kpaの代わりに認証データ {Kpm3/Cm3} Kpaがメモリカード110から出力される。その他は、上述したのと同じである。

【0124】[リッピング] パーソナルコンピュータ50のユーザは配信によって暗号化コンテンツデータとライセンスを取得する他に、所有する音楽CDから、音楽データを取得して利用することが可能である。著作権者の権利保護の立場から音楽CDのデジタル複製は自由に行なっても良いものではないが、個人が自己の使用目的のために、著作権保護機能を備えるツールを用いて複製し、音楽を楽しむことは許されている。そこで、ライセンス管理モジュール511は、音楽CDから音楽データを取得して、ライセンス管理モジュール511にて管理可能な暗号化コンテンツデータとライセンスとを生成するリッピング機能を実現するプログラムも含んでいる。

【0125】また、近年の音楽CDには、音楽データ内に、ウォーターマークと呼ばれる電子透かしを挿入したものがあある。このウォーターマークには、著作権者によって利用者における利用の範囲が利用規則として書込まれている。利用規則が書込まれている音楽データからのリッピングでは、著作権保護の点から必ずこの利用規則に従う必要がある。以後、利用規則として、複製条件(複製禁止・複製可能世代・複製可)、複製の有効期間、最大チェックアウト数、編集、再生速度、再生可能な地域のコード、複製に対する再生回数制限、利用可能時間が記載されているとする。また、ウォーターマークが検出されない場合、すなわち、利用規則が書込まれていない従来の音楽CDもある。

【0126】また、リッピングは、音楽CDから、直接、音楽データを取得する他に、アナログ信号として入力された音楽信号を、デジタル化して音楽データとして取得する場合もある。さらには、データ量を減らすために圧縮符号化された音楽データを入力することも可能である。また、さらに、本実施の形態による配信システム以外の、配信システムにて配信されたコンテンツデータを入力として取り込むことも可能である。

【0127】図12および図13を参照して、音楽データが記録された音楽CDからのリッピングによる暗号化コンテンツデータおよびライセンスの取得について説明する。

【0128】図12は、図6に示すパーソナルコンピュータ50に含まれるCD-ROMドライブ540がCDから読出した音楽データをリッピングするソフトウェアの機能を示す機能ブロック図である。音楽データをリッピングするソフトウェアは、ウォーターマーク検出手段5400と、ウォーターマーク判定手段5401と、リマーク手段5402と、ライセンス発生手段5403と、音楽エンコーダ5404と、暗号手段5405とを備える。

【0129】ウォーターマーク検出手段5400は、音楽CDから取得した音楽データからウォーターマークを検出し、記載されている利用規則を抽出する。ウォーターマーク判定手段5401は、ウォーターマーク検出手段540

10

20

30

40

50

0の検出結果、すなわち、ウォーターマークが検出できたか否か、さらに検出できた場合には、ウォーターマークで記載されていた利用規則に基づいて、リッピングの可否を判定する。この場合、リッピング可の場合、ウォーターマークの利用規則が無い、または音楽CDに記録された音楽データの複製および移動が許可された利用規則がウォーターマークによって記録されていたことを意味し、リッピング不可の場合、音楽CDに記録された音楽データを複製および移動してはいけない利用規則がウォーターマークによって記録されていたことを意味する。

【0130】リマーク手段5402は、ウォーターマーク判定手段5401における判定結果がリッピング可能で、複製世代の指示がある場合、つまり、音楽データを複製・移動して良い場合、音楽データに含まれるウォーターマークを音楽データの複製条件を変更したウォーターマークに付け替える。ただし、アナログ信号を入力してリッピングする場合や符号化された音楽データを入力とする場合、および他の配信システムにて配信された音楽データを入力とする場合には、リッピング可能であれば利用規則の内容に関わらず、必ず、ウォーターマークを付け替える。この場合、複製世代の指示がある場合は、利用規則の内容を変更して、それ以外の場合には取得した利用規則をそのまま利用する。

【0131】ライセンス発生手段5403は、ウォーターマーク判定手段5401の判定結果に基づいてライセンスを発生させる。音楽エンコーダ5404は、リマーク手段5402によってウォーターマークがリマークされた音楽データを所定の方式に符号化する。暗号手段5405は、音楽エンコーダ5404からの音楽データをライセンス発生手段5403により発生されたライセンスに

含まれるライセンス鍵Kcによって暗号化する。
【0132】図13を参照して、パーソナルコンピュータ50のコントローラ510におけるリッピング動作について説明する。リッピング動作が開始されると、ウォーターマーク検出手段5400は、音楽CDから検出したデータに基づいてウォーターマークの利用規則を検出する(ステップS800)。そして、ウォーターマーク判定手段5401は、ウォーターマーク検出手段5400の検出結果とウォーターマークとして記録されていた利用規則に基づいて複製が可能か否かを判定する(ステップS802)。ウォーターマークが検出され、利用規則によって複製が許可され、かつ、利用規則の内容がライセンス内のアクセス制御情報や再生制御情報にて対応可能な場合、リッピング可と判断され、ステップS804へ移行する。また、ウォーターマークが検出され、利用規則によって複製の禁止、または、ライセンス内のアクセス制御情報や再生制御情報にて対応不可の利用規則が記載されている場合、リッピング禁止と判断され、ステップS828へ移行してリッピング動作は終了する。装着されたCDにウォーターマークが含まれていない場合、ステップS

810へ移行する。

【0133】ステップS802において、リッピング可と判断した場合、音楽CDから音楽データが取込まれ、リマーク手段5402によって音楽データに含まれるウォーターマークが複製条件を変更したウォーターマークに付け替えられる(ステップS806)。すなわち、ウォーターマークの利用規則が3世代までの複製を許可している場合、複製世代を2回にしたウォーターマークに付け替える。そして、ライセンス発生手段5403は、利用規則を反映したライセンスを生成する。すなわち、ライセンス発生手段5403は、複製回数が2世代であるライセンスを生成する(ステップS806)。

【0134】一方、ステップS802において、ウォーターマークが検出されない場合、ライセンス発生手段5403は、ライセンスの複製のみを禁止した移動・複製制御情報が「2」のライセンスを生成する(ステップS810)。

【0135】ステップS806またはS810の後、音楽エンコーダ5404は、ウォーターマークがリマークされた音楽データを所定の方式に符号化してコンテンツデータDcを生成する(ステップS814)。そして、暗号手段5405は、音楽エンコーダ5404からの音楽データをライセンス発生手段5403により発生されたライセンスに含まれるライセンス鍵Kcによって暗号化を行ない、暗号化コンテンツデータ{Dc}Kcを生成する(ステップS816)。その後、音楽CDに含まれる情報またはパーソナルコンピュータ50のキーボード560から入力されたユーザ入力等によってコンテンツデータ{Dc}の付加情報Dc-infが生成される(ステップS818)。

【0136】そうすると、パーソナルコンピュータ50のコントローラ510は、バスBS2を介して暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを取得し、HDD530に記録する(ステップS820)。そして、コントローラ510は、生成されたライセンス(トランザクションID、コンテンツID、ライセンス鍵Kc、アクセス制限情報ACm、再生制御情報ACp)をライセンス管理デバイス520に格納する(ステップS822)。ライセンス管理デバイス520へのライセンスの格納は、コントローラ510上で実行されているライセンス管理モジュール511を介して図10および図11に示すフローチャートのステップS104からステップS166に従って行なわれる。すなわち、暗号化コンテンツデータおよびライセンスの配信における説明において配信サーバ10をコントローラ510に代えればよく、コントローラ510上で動作中のライセンス管理モジュール511は、配信サーバ10におけるライセンスの配信に対応する機能を実現できるプログラムである。その後、コントローラ510は、平文のトランザクションIDおよびコンテンツIDを含み、か

つ、HDDに記録した暗号化コンテンツデータ {Dc} Kcと付加情報Dc-infに対するライセンス管理ファイルを生成し、HDD530に記録する(ステップS824)。最後に、コントローラ510は、HDD530に記録されているコンテンツリストファイルに受理したコンテンツのファイル名を追記して(ステップS826)、リッピング動作が終了する(ステップS828)。

【0137】このように音楽CDからリッピングによっても暗号化コンテンツデータとライセンスとを取得でき、取得されたライセンスは、配信サーバ10から配信されたコンテンツとともに保護されて管理される。

【0138】このように、音楽CDからリッピングによって取得された暗号化コンテンツデータおよびライセンスは、ライセンス管理モジュール511によって生成され、配信サーバ10から受信した暗号化コンテンツデータおよびライセンスと同じように管理される。したがって、パーソナルコンピュータ50は、音楽CDからリッピングによって取得した暗号化コンテンツデータおよびライセンスを、後述するチェックアウトによって携帯電話機100または再生端末102に装着されたメモリカード110へ送信可能である。これによって、携帯電話機100または再生端末102のユーザは、パーソナルコンピュータ50がリッピングによって取得した暗号化コンテンツデータを自己のメモリカード110に受信して再生を楽しむことができる。

【0139】上記においては、パーソナルコンピュータ50は、音楽CDからリッピングによって暗号化コンテンツデータおよびライセンスを取得したが、本発明においては、これに限らず、他のインターネット配信によって受信したコンテンツデータからリッピングによって暗号化コンテンツデータおよびライセンスを生成しても良い。

【0140】〔移動〕上述したように、メモリカード110およびライセンス管理デバイス520は、配信サーバ10から暗号化コンテンツデータおよびライセンスを取得できる。そこで、メモリカード110またはライセンス管理デバイス520が配信サーバ10から受信したライセンスを他のメモリカードへ移動するときの動作について説明する。

【0141】図14および図15は、図1および図2に示すデータ配信システムにおいて、ライセンス管理デバイス520が配信サーバ10から受信した暗号化コンテンツデータおよびライセンスを携帯電話機100または再生端末102に装着されたメモリカード110へ移動する動作を説明するための第1および第2のフローチャートである。携帯電話機100または再生端末102は、移動においては、データの中継を行なうのみの機器であるため、フローチャートから省略してある。移動を説明するに当たり、図1の携帯電話機100に装着され

たメモリカード110へ移動する場合について説明を行なうが、図2の再生端末102に装着されたメモリカード110へ移動する場合についても同様であり、携帯電話機100を再生端末102に読替えれば良い。また、メモリカード110からライセンス管理デバイス520へ移動する場合も同様に、ライセンス管理デバイス520とメモリカード110とを読替えればよい。

【0142】なお、図14における処理以前に、パーソナルコンピュータ50のユーザは、コンテンツリストファイルに従って、移動するコンテンツを決定し、コンテンツファイルおよびライセンス管理ファイルが特定できていることを前提として説明する。また、コントローラ510は、ライセンス管理ファイルを保持していることを前提としている。

【0143】図14を参照して、パーソナルコンピュータ50のキーボード560から移動リクエストが入力されると(ステップS300)、コントローラ510は、USBインタフェース550、端子580、およびUSBケーブル70を介して認証データの送信要求をメモリカード110へ送信する(ステップS302)。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介して認証データの送信要求を受信する(ステップS304)。

【0144】コントローラ1420は、認証データの送信要求を受信すると、認証データ保持部1400から認証データ {K P m 3 / / C m 3} K P a をバスBS4を介して読出し、その読出した認証データ {K P m 3 / / C m 3} K P a をバスBS4、インタフェース1424および端子1426を介して外部へ出力する(ステップS306)。そして、パーソナルコンピュータ50のコントローラ510は、端子580およびUSBインタフェース550を介して認証データ {K P m 3 / / C m 3} K P a を受取り、バスBS2を介してライセンス管理デバイス520へ認証データ {K P m 3 / / C m 3} K P a を送信する(ステップS308)。

【0145】そうすると、ライセンス管理デバイス520のコントローラ5220は、端子5226およびインタフェース5224を介して認証データ {K P m 3 / / C m 3} K P a を受信し、その受信した認証データ {K P m 3 / / C m 3} K P a をバスBS5を介して復号処理部5208へ与える。そして、復号処理部5208は、K P a 保持部5214からの認証鍵K P a によって認証データ {K P m 3 / / C m 3} K P a の復号処理を実行する(ステップS310)。コントローラ5220は、復号処理部5208における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード110が正規のメモリカードからのクラス公開暗号鍵K P m 3 とクラス証明書C m 3 とを保持することを認証するために、正規の機関でその正当性を証明するための暗

号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS312)。正当な認証データであると判断された場合、コントローラ5220は、クラス公開暗号鍵K P m 3およびクラス証明書C m 3を承認し、受理する。そして、次の処理(ステップS314)へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵K P m 3およびクラス証明書C m 3を受理しないで処理を終了する(ステップS374)。

【0146】認証の結果、正当な認証データを持つメモリカードであることが確認されると、ライセンス管理デバイス520において、コントローラ5220は、セッションキー発生部5218を制御し、セッションキー発生部5218は、移動のためのセッションキーK s 2 aを生成する(ステップS314)。セッションキーK s 2 aは、復号処理部5208によって得られたメモリカード110に対応するクラス公開暗号鍵K P m 3によって、暗号化処理部5210によって暗号化される。そして、コントローラ5220は、バスB S 5を介して暗号化データ{K s 2 a} K m 3を取得し、バスB S 5、インタフェース5224および端子5226を介して暗号化データ{K s 2 a} K m 3を出力する(ステップS316)。

【0147】コントローラ510は、バスB S 2を介して{K s 2 a} K m 3をライセンス管理デバイス520から受理し(ステップS318)、HDD530に記録されているライセンス管理情報からライセンスIDを取得する(ステップS320)。そして、コントローラ510は、取得したライセンスIDと、ステップS318において受理した暗号化データ{K s 2 a} K m 3とを1つのデータにしてライセンスID//{K s 2 a} K m 3を端子580およびUSBインタフェース550を介して携帯電話機100に装着されたメモリカード110へ送信する(ステップS322)。そうすると、メモリカード110のコントローラ1106は、端子1426、インタフェース1424、およびバスB S 4を介してライセンスID//{K s 2 a} K m 3を受理する(ステップS324)。その後、コントローラ1420は、暗号化データ{K s 2 a} K m 3を復号処理部1422へ与え、復号処理部1422は、K m 保持部1421からのクラス秘密復号鍵K m 3によって{K s 2 a} K m 3を復号してセッションキーK s 2 aを受理する(ステップS326)。そして、セッションキー発生部1418は、セッションキーK s 2 bを生成し(ステップS328)、暗号化処理部1406は、切換スイッチ1446の端子を順次切換えることによって取得したセッションキーK s 2 b、および個別公開暗号鍵K P m c 4を、復号処理部1404によって復号されたセッションキーK s 2 aによって暗号化し、暗号化データ{K s 2 b//K P m c 4} K s 2 aを生成する。コントローラ1420は、暗号化データ{K s 2 b//K P m c 4} K s 2 aをバスB S 4、インタフェース1424および端子1426を介して出力し(ステップS330)、パーソナルコンピュータ50のコントローラ510は、端子580およびUSBインタフェース550を介して暗号化データ{K s 2 b//K P m c 4} K s 2 aを受理する。そして、コントローラ510は、暗号化データ{K s 2 b//K P m c 4} K s 2 aをバスB S 2を介してライセンス管理デバイス520へ送信する(ステップS332)。

【0148】そうすると、ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224およびバスB S 5を介して暗号化データ{K s 2 b//K P m c 4} K s 2 aを受信し、その受信した暗号化データ{K s 2 b//K P m c 4} K s 2 aを復号処理部5212に与える。復号処理部5212は、セッションキー発生部5218からのセッションキーK s 2 aによって暗号化データ{K s 2 b//K P m c 4} K s 2 aを復号し、セッションキーK s 2 b、および公開暗号鍵K P m c 4を受理する(ステップS334)。

【0149】その後、コントローラ510は、ライセンス管理デバイス520に対応するライセンス管理情報から移動の対象となっているライセンスが格納されているエントリ番号を取得し(ステップS336)、その取得したエントリ番号とライセンスの移動要求とをライセンス管理デバイス520へ入力する(ステップS338)。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224、およびバスB S 5を介してエントリ番号とライセンスの移動要求とを受信し、その受信したエントリ番号によって指定されるメモリ5215のライセンス領域5215Aのエントリからライセンス(ライセンスID、コンテンツID、ライセンス鍵K c、アクセス制御情報A C m、再生制御情報A C p)を取得する(ステップS340)。

【0150】図15を参照して、コントローラ5220は、ステップS340において取得したライセンスの貸出の有無を貸出フラグによって判定する(ステップS342)。そして、取得したライセンスが貸出中であれば、移動動作は終了する(ステップS374)。取得したライセンスが貸出中でなければ、コントローラ5220は、次いで、アクセス制御情報A C mを確認する(ステップS344)。つまり、コントローラ5220は、取得したアクセス制御情報A C mに基づいて、最初に、メモリカード110へ移動しようとするライセンスが再生回数によって暗号化コンテンツデータの再生ができないライセンスになっていないか否かを確認する。再生回数が残っていない場合(再生回数=0)、暗号化コンテンツデータをライセンスによって再生することができ

ず、その暗号化コンテンツデータとライセンスとをメモリカード110へ移動する意味がないからである。再生することができない場合、再生することができる場合、移動・複製制御情報によって、ライセンスの複製、移動の可否を判断する。

【0151】ステップS344において、暗号化コンテンツデータの再生回数ができない(再生回数=0)、または、移動・複製フラグが移動複製禁止(=0)の場合、アクセス制御情報ACmによって、複製移動不可と判断し、ステップS374へ移行し、移動動作は終了する。ステップS344において、暗号化コンテンツデータの再生ができ(再生回数≠0)、かつ、移動・複製制御情報が移動のみ可「=2」の場合、ライセンスの移動であると判断され、コントローラ5220は、メモリ5215のライセンス領域5215Aにおいて指定されたエントリ番号内の有効フラグを無効する(ステップS346)。また、暗号化コンテンツデータの再生ができ「再生回数≠0」、かつ、移動・複製制御情報が複製可の場合、ライセンスの複製であると判断され、ステップS346を行わずにステップS348へ移行する。

【0152】ステップS344またはステップS346の後、暗号化処理部5217は、復号処理部5212によって得られたメモリカード110に固有の公開暗号鍵Kpmc4によってライセンスを暗号化して暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を生成する(ステップS348)。このように、ライセンスの移動が可能となるときは、ライセンス領域5215Aの有効フラグを無効にしてから(ステップS346参照)、ステップS348の処理を行なうが、ライセンスの複製が許可されている場合は、複製元と複製先との両方においてライセンスを使用可能にするためにライセンスの有効フラグを無効にするステップS346を介さずにステップS348へ移行するようにしたものである。したがって、ライセンスを移動させたときは、ライセンス管理デバイス520からライセンスを読出すことはできない。

【0153】そして、暗号化処理部5206は、暗号化処理部5217によって暗号化された暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4をスイッチ5246の接点Pcを介して受取り、復号処理部5212によって復号されたセッションキーKs2bをスイッチ5242の接点Pbを介して受取り、暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4をセッションキーKs2bによって暗号化する。そして、コントローラ5220は、暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bをバスBS5、インタフェース5224、および端子5226を介して出力する(ステップS350)。

【0154】コントローラ510は、バスBS2を介してメモリカード120から暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bを受取り、その受取した暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bをメモリカード110へ送信する(ステップS352)。

【0155】メモリカード110のコントローラ1420は、端子1426、インタフェース1424、およびバスBS4を介して暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bの入力を受けて、暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bを復号処理部1412へ与える。そして、復号処理部1412は、暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bをバスBS4を介して受取り、セッションキー発生部1418によって発生されたセッションキーKs2bによって復号し、{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を受理する(ステップS354)。

【0156】その後、コントローラ1420の指示によって、暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4は、復号処理部1404において、秘密復号鍵Kmc4によって復号され、ライセンス(ライセンス鍵Kc、ライセンスID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp)が受理される(ステップS356)。

【0157】そうすると、コントローラ510は、受信側であるメモリカード110のライセンス管理情報から移動/複製されたライセンスを格納するためのエントリ番号を決定し、メモリカード110に入力するとともに、受信側(メモリカード110)のライセンス管理情報を更新する(ステップS358)。

【0158】そうすると、メモリカード100のコントローラ1420は、ステップS356において取得したアクセス制御情報ACmに基づいて、取得したライセンスが貸出可能か否かを判定する(ステップS360)。

そして、コントローラ1420は、ライセンスの貸出が可能であれば、メモリ1415のライセンス領域1415Aのエントリ番号によって指定された領域に格納された貸出フラグを「可」に設定する(ステップS362)。一方、ステップS360において、ライセンスの貸出が不可と判定されたとき、コントローラ1420は、ライセンス領域1415Aのエントリ番号によって指定された領域に格納された貸出フラグを「不可」に設定する(ステップS364)。

【0159】ステップS362またはステップS364の後、コントローラ1420は、ライセンス領域141

10

20

30

40

50

5 Aのエントリ番号によって指定された領域に格納された有効フラグを「有効」に設定し(ステップS 366)、ライセンス領域1415 Aのエントリ番号によって指定された領域に、ステップS 356において受理したライセンス(ライセンスID、コンテンツID、ライセンス鍵Kc、アクセス制御情報ACm、および再生制御情報ACp)を格納する(ステップS 368)。

【0160】一方、ステップS 358の後、コントローラ510は、ライセンスの移動または複製が可能か否かを判定し(ステップS 370)、移動可能であるとき、送信側のライセンス管理情報、すなわち、移動したライセンスに対応するHDD530に記録されているライセンス管理情報を削除し、送信側のライセンス管理情報およびメモリカード110のデータ領域1415 Bに記録されているライセンス管理ファイルを書換える(ステップS 372)。ステップS 370において、ライセンスの貸出が可能と判定されたとき、またはステップS 372の後、またはステップS 368の後、ライセンスの移動動作は終了する(ステップS 374)。

【0161】なお、暗号化コンテンツデータのメモリカード120からメモリカード110への移動は、ライセンスの移動が終了した後、メモリカード120のデータ領域1415 Bから暗号化コンテンツデータを読み出してメモリカード110へ送信することによって行なえば良い。

【0162】このようにして、携帯電話機100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cm3とともに暗号化して送信できた公開暗号鍵Kpm3が有効であることを確認した上で、正規なメモリカードへの移動要求に対してのみライセンスを移動することができ、不正なメモリカードへの移動を禁止することができる。

【0163】また、メモリカードで生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、ライセンスの移動の動作におけるセキュリティを向上させることができる。

【0164】また、メモリカード110からライセンス管理デバイス520へのライセンスの移動も、図14および図15に示すフローチャートに従って行なわれる。つまり、図1において、携帯電話機100によって配信を受け、メモリカード110に格納した暗号化コンテンツデータとライセンスとをパーソナルコンピュータ50へ退避できることになる。

【0165】また、パーソナルコンピュータ50が配信サーバ10から受信したライセンスをメモリカード110へ移動できるのは、ライセンス管理デバイス520が配信サーバ10からハード的に受信したライセンスだけ

であり、音楽CDからライセンス管理モジュール511によってリッピングされたライセンスは移動できない。そこで、次に説明するチェックアウト(貸出)およびチェックイン(返却)の概念によって、ライセンス管理モジュール511によってリッピングし、ライセンス管理デバイス520に記録したライセンスをメモリカード110へ送信できるようにした。

【0166】また、メモリカード120からメモリカード110へのライセンスの貸出、および返却も可能である。「移動」と「貸出」との相違は、「移動」は、ライセンスを移動させた送信元のメモリカードにおいては、ライセンスの有効フラグが無効に設定されている(図15のステップS 346参照)ため、「移動」は、送信元のメモリカードから暗号化コンテンツデータおよびライセンスを取得して暗号化コンテンツデータの再生を行なうことができないが、「貸出」は、ライセンスを貸出した貸出元のメモリカードから暗号化コンテンツデータおよびライセンスを取得して暗号化コンテンツデータの再生を行なうことができる点にある。また、上述したように、音楽CDからリッピングしたライセンスを送る。

【0167】[貸出] 図1および図2に示すデータ配信システムにおいて、配信サーバ10からライセンス管理デバイス520へ配信された、あるいは音楽CDからリッピングされた暗号化コンテンツデータおよびライセンスをメモリカード110に返却を前提として貸出するために送信する動作について説明する。なお、この動作を「貸出」という。

【0168】図16および図17は、ライセンス管理デバイス520からメモリカード110へのライセンスの貸出を説明するための第1および第2のフローチャートである。

【0169】なお、図16における処理以前に、携帯電話機100のユーザは、コンテンツリストファイルに従って、移動するコンテンツを決定し、コンテンツファイルおよびライセンス管理ファイルが特定できていることを前提として説明する。また、コントローラ40は、ライセンス管理ファイルを保持していることを前提としている。

【0170】図16を参照して、パーソナルコンピュータ50のキーボード560から貸出リクエストが入力されると(ステップS 400)、コントローラ510は、携帯電話機100を介して認証データの送信要求をメモリカード110へ送信する(ステップS 402)。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介して認証データの送信要求を受信する(ステップS 404)。

【0171】コントローラ1420は、認証データの送信要求を受信すると、認証データ保持部1400から認証データ{Kpm3/／Cm3} KPaをバスBS4を

介して読出し、その読出した認証データ {K P m 3 / / C m 3} K P a をバス B S 4、インタフェース 1 4 2 4 および端子 1 4 2 6 を介して外部へ出力する (ステップ S 4 0 6)。そして、パーソナルコンピュータ 5 0 のコントローラ 5 1 0 は、端子 5 8 0 および U S B インタフェース 5 5 0 を介して認証データ {K P m 3 / / C m 3} K P a を受取り、バス B S 2 を介してライセンス管理デバイス 5 2 0 へ認証データ {K P m 3 / / C m 3} K P a を送信する (ステップ S 4 0 8)。

【0172】そうすると、ライセンス管理デバイス 5 2 0 のコントローラ 5 2 2 0 は、端子 5 2 2 6 およびインタフェース 5 2 2 4 を介して認証データ {K P m 3 / / C m 3} K P a を受信し、その受信した認証データ {K P m 3 / / C m 3} K P a をバス B S 5 を介して復号処理部 5 2 0 8 へ与える。そして、復号処理部 5 2 0 8 は、K P a 保持部 5 2 1 4 からの認証鍵 K P a によって認証データ {K P m 3 / / C m 3} K P a の復号処理を実行する (ステップ S 4 1 0)。コントローラ 1 4 2 0 は、復号処理部 5 2 0 8 における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード 1 1 0 が正規のメモリカードからのクラス公開暗号鍵 K P m 3 とクラス証明書 C m 3 とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう (ステップ S 4 1 2)。正当な認証データであると判断された場合、コントローラ 5 2 2 0 は、クラス公開暗号鍵 K P m 3 およびクラス証明書 C m 3 を承認し、受理する。そして、次の処理 (ステップ S 4 1 4) へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵 K P m 3 およびクラス証明書 C m 3 を受理しないで処理を終了する (ステップ S 4 7 8)。

【0173】認証の結果、正当な認証データを持つメモリカードからのアクセスであることが確認されると、ライセンス管理デバイス 5 2 0 において、コントローラ 5 2 2 0 は、セッションキー発生部 5 2 1 8 を制御し、セッションキー発生部 5 2 1 8 は、貸出のためのセッションキー K s 2 a を生成する (ステップ S 4 1 4)。セッションキー K s 2 a は、復号処理部 5 2 0 8 によって得られたメモリカード 1 1 0 に対応するクラス公開暗号鍵 K P m 3 によって、暗号化処理部 5 2 1 0 によって暗号化される。そして、コントローラ 5 2 2 0 は、バス B S 5 を介して暗号化データ {K s 2 a} K m 3 を取得し、バス B S 5、インタフェース 5 2 2 4 および端子 5 2 2 6 を介して暗号化データ {K s 2 a} K m 3 を出力する (ステップ S 4 1 6)。

【0174】コントローラ 5 1 0 は、バス B S 2 を介して {K s 2 a} K m 3 を送信側から受理し (ステップ S 4 1 8)、送信側のライセンス管理情報、すなわち、H D D 5 3 0 に記録されている貸出を行なうライセンスに

対応するライセンス I D を取得する (ステップ S 4 2 0)。そして、コントローラ 5 1 0 は、取得したライセンス I D と、ステップ S 4 1 8 において受理した暗号化データ {K s 2 a} K m 3 とを 1 つにデータにしてライセンス I D / / {K s 2 a} K m 3 を端子 5 8 0 および U S B インタフェース 5 5 0 を介してメモリカード 1 1 0 へ送信する (ステップ S 4 2 2)。そうすると、メモリカード 1 1 0 のコントローラ 1 4 2 0 は、端子 1 4 2 6、インタフェース 1 4 2 4、およびバス B S 4 を介してライセンス I D / / {K s 2 a} K m 3 を受理する (ステップ S 4 2 4)。その後、コントローラ 1 4 2 0 は、暗号化データ {K s 2 a} K m 3 を復号処理部 1 4 2 2 へ与え、復号処理部 1 4 2 2 は、K m 保持部 1 4 2 1 からのクラス秘密復号鍵 K m 3 によって {K s 2 a} K m 3 を復号してセッションキー K s 2 a を受理する (ステップ S 4 2 6)。そして、セッションキー発生部 1 4 1 8 は、セッションキー K s 2 b を生成し (ステップ S 4 2 8)、暗号化処理部 1 4 0 6 は、切換スイッチ 1 4 4 6 の端子を順次切換えることによって取得したセッションキー K s 2 b、および個別公開暗号鍵 K P m c 4 を、復号処理部 1 4 0 4 によって復号されたセッションキー K s 2 a によって暗号化し、暗号化データ {K s 2 b / / K P m c 4} K s 2 a を生成する。コントローラ 1 4 2 0 は、暗号化データ {K s 2 b / / K P m c 4} K s 2 a をバス B S 4、インタフェース 1 4 2 4 および端子 1 4 2 6 を介して出力し (ステップ S 4 3 0)、コントローラ 5 1 0 は、端子 5 8 0 および U S B インタフェース 5 5 0 を介して暗号化データ {K s 2 b / / K P m c 4} K s 2 a を受理する。そして、コントローラ 5 1 0 は、暗号化データ {K s 2 b / / K P m c 4} K s 2 a をバス B S 2 を介してライセンス管理デバイス 5 2 0 へ入力する (ステップ S 4 3 2)。

【0175】そうすると、ライセンス管理デバイス 5 2 0 のコントローラ 5 2 2 0 は、端子 5 2 2 6、インタフェース 5 2 2 4 およびバス B S 5 を介して暗号化データ {K s 2 b / / K P m c 4} K s 2 a を受信し、その受信した暗号化データ {K s 2 b / / K P m c 4} K s 2 a を復号処理部 5 2 1 2 に与える。復号処理部 5 2 1 2 は、セッションキー発生部 5 2 1 8 からのセッションキー K s 2 a によって暗号化データ {K s 2 b / / K P m c 4} K s 2 a を復号し、セッションキー K s 2 b、および公開暗号鍵 K P m c 4 を受理する (ステップ S 4 3 4)。

【0176】その後、コントローラ 5 1 0 は、貸出を行なうライセンスに対応したライセンス管理情報から移動の対象となっているライセンスが格納されているエントリ番号を取得し (ステップ S 4 3 6)、貸出用ライセンス I D を生成し (ステップ S 4 3 8)、ステップ S 4 3 6 において取得したエントリ番号とステップ S 4 3 8 において生成した貸出用ライセンス I D とによって指定さ

れたライセンスの貸出要求をライセンス管理デバイス520へ入力する(ステップS440)。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224、およびバスBS5を介してエントリ番号、貸出用ライセンスID、およびライセンスの貸出要求とを受信し、その受信したエントリ番号によって指定されるメモリ1415のライセンス領域5215Aのエントリからライセンス(ライセンスID、コンテンツID、ライセンス鍵Kc、アクセス制御情報ACm、再生制御情報ACp)を取得する(ステップS442)。

【0177】コントローラ5220は、取得したアクセス制御ACmによってライセンスの複製が可能か否かを判定し(ステップS444)、複製可であれば図17のステップS452へ移行し、複製が禁止されていれば図17のステップS446へ移行する。

【0178】図17を参照して、ステップS444においてライセンスの複製が禁止されていると判定されたとき、ステップS442において取得したライセンスの貸出可否を貸出フラグによって判定する(ステップS446)。そして、取得したライセンスが貸出不可であれば、貸出動作は終了する(ステップS478)。取得したライセンスが貸出可でなければ、コントローラ5220は、指定されたエントリ内の貸出フラグを「貸出中」に変更し、受理した貸出用ライセンスIDを貸出時ライセンスIDの欄に格納し、ステップS434において受理した公開暗号鍵Kpmc4を貸出先IDの欄に格納する(ステップS448)。そして、コントローラ5220は、移動・複製禁止を設定した(移動・複製制御情報が「3」である)貸出用アクセス制御情報ACmを生成し、受理した貸出用ライセンスIDと生成した貸出用アクセス制御情報ACmとを、指定されたエントリから取得したライセンスIDおよびアクセス制御情報ACmと置換する(ステップS450)。これによって、メモリカード110へ貸出されるライセンス(貸出用ライセンスID、コンテンツID、ライセンス鍵Kc、貸出用アクセス制御情報ACm、再生制御情報ACp)が生成されるとともに、ライセンス管理デバイス520のメモリ5215のライセンス領域5215Aには、元のライセンス(貸出用ライセンスID、コンテンツID、ライセンス鍵Kc、貸出用アクセス制御情報ACm、再生制御情報ACp)が格納されたままである。そして、ライセンス管理デバイス520のライセンス領域5215Aに格納されたままのライセンスは、メモリカード110へ貸出される。このため、ライセンス管理デバイス520には、移動の場合と異なりライセンスが残るためライセンスのバックアップとして機能する。

【0179】ステップS444において複製可と判定されたとき、またはステップS450の後、暗号化処理部5217は、復号処理部5212によって得られたメモ

リカード110に固有の公開暗号鍵Kpmc4によってライセンスを暗号化して暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を生成する(ステップS452)。なお、ステップS444においてライセンスの複製が可能と判定されたとき、ステップS442において取得されたライセンスが公開暗号鍵Kpmc4によって暗号化される。

【0180】そして、暗号化処理部5206は、暗号化処理部5217によって暗号化された暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4をスイッチ5246の接点Pcを介して受取り、復号処理部5212によって復号されたセッションキーKs2bをスイッチ5242の接点Pbを介して受取り、暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4をセッションキーKs2bによって暗号化する。そして、コントローラ5220は、暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bをバスBS5、インタフェース5224、および端子5226を介して出力する(ステップS454)。

【0181】コントローラ510は、バスBS2を介してメモリカード120から暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bを受取り、その受理した暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bを携帯電話機100に装着された貸出先のメモリカード110へ入力する(ステップS456)。

【0182】メモリカード110のコントローラ1420は、端子1426、インタフェース1424、およびバスBS4を介して暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bの入力を受けて、暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bを復号処理部1412へ与える。そして、復号処理部1412は、暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bをバスBS4を介して受取り、セッションキー発生部1418によって発生されたセッションキーKs2bによって復号し、{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を受理する(ステップS458)。

【0183】その後、コントローラ1420の指示によって、暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4は、復号処理部1404において、秘密復号鍵Kmc4によって復号され、ライセンス(ライセンス鍵Kc、ライセンスID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp)が受理される(ステップS46

0)。

【0184】そうすると、コントローラ510は、受信側であるメモリカード110のライセンス管理情報から移動/複製されたライセンスを格納するためのエントリ番号を決定し、メモリカード110に入力するとともに、受信側のライセンス管理情報を更新する(ステップS462)。

【0185】そうすると、メモリカード100のコントローラ1420は、ステップS460において取得したアクセス制御情報ACmに基づいて、取得したライセンスが貸出可能か否かを判定する(ステップS464)。そして、コントローラ1420は、ライセンスの貸出が可能であれば、メモリ1415のライセンス領域1415Aのエントリ番号によって指定された領域に格納された貸出フラグを「可」に設定する(ステップS466)。一方、ステップS360において、ライセンスの貸出が不可と判定されたとき、コントローラ1420は、ライセンス領域1415Aのエントリ番号によって指定された領域に格納された貸出フラグを「不可」に設定する(ステップS468)。貸出においては、ステップS450においてアクセス制御情報の移動・複製制御情報が移動・複製不可に設定されてライセンス管理デバイス520から出力されるため必ずステップS468へ進む。

【0186】ステップS466またはステップS468の後、コントローラ1420は、ライセンス領域1415Aのエントリ番号によって指定された領域に格納された有効フラグを「有効」に設定し(ステップS470)、ライセンス領域1415Aのエントリ番号によって指定された領域に、ステップS460において受理したライセンス(ライセンスID、コンテンツID、ライセンス鍵Kc、アクセス制御情報ACm、および再生制御情報ACp)を格納する(ステップS472)。

【0187】一方、ステップS462の後、コントローラ510は、ライセンスの移動または複製が可能か否かを判定し(ステップS474)、移動可能であるとき、貸出先のライセンス管理情報に貸出用ライセンスIDを追記し、貸出先ライセンス管理情報を更新する(ステップS476)。ステップS474において、ライセンスの貸出が可能と判定されたとき、またはステップS476の後、またはステップS472の後、ライセンスの貸出動作は終了する(ステップS478)。

【0188】なお、暗号化コンテンツデータのメモリカード110への貸出は、ライセンスの移動が終了した後、コントローラ510がHDD530から暗号化コンテンツデータを読み出してメモリカード110へ送信することによって行なえば良い。

【0189】このようにして、携帯電話機100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cm3とともに暗号化して送信でき

た公開暗号鍵Kpm3が有効であることを確認した上で、正規なメモリカードへの貸出要求に対してのみライセンスを貸出を行なうことができ、不正なメモリカードへの貸出を禁止することができる。

【0190】また、メモリカードで生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、ライセンスの貸出動作におけるセキュリティを向上させることができる。

【0191】[返却] 図16および図17を参照して説明したライセンス管理デバイス520からメモリカード110へ貸出されたライセンスをメモリカード110からライセンス管理デバイス520へ返却する動作について説明する。

【0192】図18～図21は、メモリカード110からライセンス管理デバイス520へライセンスを返却する動作を説明するための第1～第4のフローチャートである。

【0193】なお、図18における処理以前に、ユーザは、パーソナルコンピュータ50にUSBケーブル70によって接続された携帯電話機100に装着されたメモリカード110から返却されるライセンスおよびコンテンツをHDD530に記録されているコンテンツリストファイルに従って決定し、返却側のコンテンツファイルと貸出側および返却側の双方のライセンス管理ファイルとが特定できていることを前提として説明する。

【0194】図18を参照して、パーソナルコンピュータ50のキーボード560から返却リクエストが入力されると(ステップS500)、コントローラ510は、端子580およびUSBインタフェース550を介して認証データの送信要求をメモリカード110へ送信する(ステップS502)。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスB4を介して認証データの送信要求を受信する(ステップS504)。

【0195】コントローラ1420は、認証データの送信要求を受信すると、認証データ保持部1400から認証データ{Kpm3//Cm3}KPaをバスB4を介して読出し、その読出した認証データ{Kpm3//Cm3}KPaをバスB4、インタフェース1424および端子1426を介してコントローラ510へ出力する(ステップS506)。そして、コントローラ510は、端子580およびUSBインタフェース550を介して認証データ{Kpm3//Cm3}KPaを受取り、バスB2を介してライセンス管理デバイス520へ認証データ{Kpm3//Cm3}KPaを送信する(ステップS508)。

【0196】そうすると、ライセンス管理デバイス520のコントローラ5220は、端子5226およびイン

タフェース5224を介して認証データ {K P m 3 / / C m 3} K P aを受信し、その受信した認証データ {K P m 3 / / C m 3} K P aをバスB S 5を介して復号処理部5208へ与える。そして、復号処理部5208は、K P a保持部5214からの認証鍵K P aによって認証データ {K P m 3 / / C m 3} K P aの復号処理を実行する(ステップS 510)。コントローラ5220は、復号処理部5208における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード110が正規のメモリカードからのクラス公開暗号鍵K P m 3とクラス証明書C m 3とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS 512)。正当な認証データであると判断された場合、コントローラ5220は、クラス公開暗号鍵K P m 3およびクラス証明書C m 3を承認し、受理する。そして、次の処理(ステップS 514)へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵K P m 3およびクラス証明書C m 3を受理しないで処理を終了する(ステップS 638)。

【0197】認証の結果、正当な認証データを持つメモリカードを備える再生端末からのアクセスであることが確認されると、ライセンス管理デバイス520において、コントローラ5220は、セッションキー発生部5218を制御し、セッションキー発生部5218は、返却のためのセッションキーK s 2 aを生成する(ステップS 514)。セッションキーK s 2 aは、復号処理部5208によって得られたメモリカード110に対応するクラス公開暗号鍵K P m 3によって、暗号化処理部1410によって暗号化される。そして、コントローラ5220は、バスB S 5を介して暗号化データ {K s 2 a} K m 3を取得し、バスB S 5、インタフェース5224および端子5226を介して暗号化データ {K s 2 a} K m 3を出力する(ステップS 516)。

【0198】コントローラ510は、バスB S 2を介して {K s 2 a} K m 3をライセンス管理デバイス520から受理し(ステップS 518)、貸出元のライセンス管理情報から貸出時のライセンスIDを取得する(ステップS 520)。そして、コントローラ40は、取得したライセンスIDと、ステップS 518において受理した暗号化データ {K s 2 a} K m 3とを1つにデータにしてライセンスID / / {K s 2 a} K m 3をメモリカード110へ送信する(ステップS 522)。そうすると、メモリカード110のコントローラ1420は、端子1426、インタフェース1424、およびバスB S 4を介してライセンスID / / {K s 2 a} K m 3を受理する(ステップS 524)。その後、コントローラ1420は、暗号化データ {K s 2 a} K m 3を復号処理部1422へ与え、復号処理部1422は、K m 保持部

1421からのクラス秘密復号鍵K m 3によって {K s 2 a} K m 3を復号してセッションキーK s 2 aを受理する(ステップS 526)。そして、セッションキー発生部1418は、セッションキーK s 2 bを生成し(ステップS 528)、暗号化処理部1406は、切換スイッチ1446の端子を順次切換えることによって取得したセッションキーK s 2 b、および個別公開暗号鍵K P m c 4を、復号処理部1404によって復号されたセッションキーK s 2 aによって暗号化し、暗号化データ {K s 2 b / / K P m c 4} K s 2 aを生成する。コントローラ1420は、暗号化データ {K s 2 b / / K P m c 4} K s 2 aをバスB S 4、インタフェース1424および端子1426を介して出力し(ステップS 530)、コントローラ510は、端子580およびU S Bインタフェース550を介して暗号化データ {K s 2 b / / K P m c 4} K s 2 aを受理する。そして、コントローラ510は、暗号化データ {K s 2 b / / K P m c 4} K s 2 aをバスB S 2を介してライセンス管理デバイス520へ送信する(ステップS 532)。

【0199】そうすると、ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224およびバスB S 5を介して暗号化データ {K s 2 b / / K P m c 4} K s 2 aを受信し、その受信した暗号化データ {K s 2 b / / K P m c 4} K s 2 aを復号処理部5212に与える。復号処理部5212は、セッションキー発生部5218からのセッションキーK s 2 aによって暗号化データ {K s 2 b / / K P m c 4} K s 2 aを復号し、セッションキーK s 2 b、および公開暗号鍵K P m c 4を受理する(ステップS 534)。

【0200】そして、コントローラ510は、ライセンスの検索要求を貸出先のメモリカード110へ入力する(ステップS 534)。メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスB S 4を介してライセンスの検索要求を受理し(ステップS 536)、ステップS 524において受理したライセンスIDに基づいてメモリ1415のライセンス領域1415Aを検索する。そして、コントローラ1420は、検索結果s t a t eを生成する(ステップS 538)。

【0201】暗号化処理部1406は、復号処理部1412によって復号して得られたセッションキーK s 2 aをスイッチ1442の接点P bを介して受け、セッションキー発生部1418が発生したセッションキーK s 2 bをスイッチ1446の接点P dを介して受ける。そして、暗号化処理部1406は、セッションキーK s 2 bをセッションキーK s 2 aによって暗号化して暗号化データ {K s 2 b} K s 2 aを生成する(ステップS 540)。そして、コントローラ1420は、ライセンスID / / {K s 2 b} K s 2 a / / s t a t eを生成し、

その生成したライセンスID// {Ks2b} Ks2a //stateのハッシュ値hashを求める(ステップS542)。つまり、コントローラ1420は、ライセンスID// {Ks2b} Ks2a //stateの署名を行なう。その後、コントローラ1420は、ハッシュ値hashをスイッチ1446の接点Pfを介して暗号化処理部1406へ与える。暗号化処理部1406は、ハッシュ値hashをセッションキーKs2aによって暗号化し、暗号化データ{hash} Ks2aを生成する(ステップS544)。

【0202】図19を参照して、メモリカード110のコントローラ1420は、ライセンスID// {Ks2b} Ks2a //state // {hash} Ks2aを生成し、バスBS4、インタフェース1424、および端子1426を介してライセンスID// {Ks2b} Ks2a //state // {hash} Ks2aを出力する(ステップS546)。コントローラ510は、端子580およびUSBインタフェース550を介してメモリカード110からライセンスID// {Ks2b} Ks2a //state // {hash} Ks2aを受信する(ステップS548)。そして、コントローラ510は、貸出元のライセンス管理情報から返却するライセンスが格納されているエントリ番号を取得し(ステップS550)、ステップS548において取得したライセンスID// {Ks2b} Ks2a //state // {hash} Ks2aとエントリ番号を指定したライセンス返却要求とを貸出元のライセンス管理デバイス520へ入力する(ステップS552)。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224およびバスBS5を介してライセンスID// {Ks2b} Ks2a //state // {hash} Ks2aとエントリ番号とライセンス返却要求とを受信し(ステップS554)、その受信したエントリ番号によって指定された領域に格納されている貸出フラグ、貸出時のライセンスID、および貸出先IDに格納された公開暗号鍵Kpmtxを取得する(ステップS556)。

【0203】そうすると、コントローラ5220は、取得した公開暗号鍵KpmtxがステップS534において受理したメモリカード110に固有の公開暗号鍵Kpmc4に一致するか否かを判定し(ステップS558)、不一致であるとき、返却動作は終了する(ステップS638)。つまり、メモリカード110がライセンスを貸出した相手でないことが判定されたことになるので、返却動作を終了することにしたものである。公開暗号鍵Kpmtxが公開暗号鍵Kpmc4に一致したとき、コントローラ5220は、貸出フラグが貸出中になっているか否かを判定し(ステップS560)、貸出中でなければライセンスを返却する必要がないので、返却動作は終了する(ステップS638)。ステップS560にお

いてライセンスが返却中であると判定されると、コントローラ5220は、受理したライセンスIDが貸出時のライセンスIDに一致するか否かを判定し(ステップS562)、不一致であるとき、返却動作は終了する(ステップS638)。つまり、返却要求のあったライセンスのライセンスIDが貸出したライセンスのライセンスIDに一致せず、貸出したライセンスが返却されないことになるので、返却動作を終了することにしたものである。ステップS562において、2つのライセンスIDが一致したとき、コントローラ5220は、メモリカード110におけるライセンスの検索結果stateを確認する(ステップS564)。すなわち、コントローラ5220は、返却しようとするライセンスがメモリカード110のライセンス領域1415Aに本当に格納されているか否かを確認し、ライセンス領域1415Aに格納されていないとき、返却動作を終了する(ステップS638)。そして、コントローラ5220は、返却しようとするライセンスがメモリカード110のライセンス領域1415Aに格納されていることを確認したとき、ライセンスID// {Ks2b} Ks2a //stateのハッシュ値hashを求める(ステップS566)。つまり、ライセンス管理デバイス520のコントローラ5220は、自らライセンスID// {Ks2b} Ks2a //stateに対する署名を行ない、ハッシュ値hashを求める。

【0204】その後、コントローラ5220は、ステップS554において受理した{hash} Ks2aを復号処理部5212に与える。復号処理部5212は、{hash} Ks2aをセッションキーKs2aによって復号し、コントローラ5220は、メモリカード110におけるハッシュ値hashを受信する(ステップS568)。そして、コントローラ5220は、自ら求めたハッシュ値hashがメモリカード110におけるハッシュ値hashに一致するか否かを判定し(ステップS570)、不一致であるとき、メモリカード110における署名が書換えられていることになるので返却動作は終了する(ステップS638)。2つのハッシュ値が一致したとき、コントローラ5220は、ステップS554において受理した暗号化データ{Ks2b} Ks2aを復号処理部5212に与える。復号処理部5212は、暗号化データ{Ks2b} Ks2aをセッションキーKs2aによって復号してセッションキーKs2bを受信する(ステップS572)。

【0205】そして、コントローラ5220は、セッションキーKs2bの確認を行ない(ステップS574)、ライセンスの貸出時にメモリカード110から受信したセッションキーKs2bと不一致であれば返却動作は終了し(ステップS638)、一致すれば図20のステップS576へ移行する。

【0206】図20を参照して、貸出先に貸出したライ

10

20

30

40

50

センスを無効にするための無効ダミーライセンス（偽ライセンスID、偽コンテンツID、偽ライセンス鍵Kc、偽アクセス制御情報ACm、および偽再生制御情報ACp）を生成し、その生成した無効ダミーライセンスを暗号化処理部5217に与える。暗号化処理部5217は、無効ダミーライセンスを復号処理部5212によって復号された公開暗号鍵Kpmc4によって暗号化し、暗号化データ {偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp} Kmc4を生成する（ステップS576）。そして、暗号化処理部5206は、暗号化データ {偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp} Kmc4をスイッチ5246の接点Pcを介して受取り、その受取った暗号化データ {偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp} Kmc4をスイッチ5246の接点Pdを介して受取ったセッションキーKs2bによって暗号化して暗号化データ {偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp} Kmc4} Ks2bを出力する。そして、コントローラ5220は、バスBS5、インタフェース5224、および端子5226を介して暗号化データ {偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp} Kmc4} Ks2bを出力する（ステップS578）。

【0207】コントローラ510は、バスBS2を介して暗号化データ {偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp} Kmc4} Ks2bを貸出元であるライセンス管理デバイス520から受け、貸出先であるメモリカード110へ暗号化データ {偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp} Kmc4} Ks2bを送信する（ステップS580）。

【0208】メモリカード110のコントローラ1420は、端子1426、インタフェース1424、およびバスBS4を介して暗号化データ {偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp} Kmc4} Ks2bを受取り、その受取った暗号化データを復号処理部1412に与える。復号処理部1412は、暗号化データをセッションキーKs2bによって復号して {偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp} Kmc4を受取り（ステップS582）。そして、復号処理部1404は、復号処理部14

12からの暗号化データ {偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp} Kmc4をKmc保持部1402からの秘密鍵Kmc4によって復号して無効ダミーライセンス（偽ライセンスID//偽コンテンツID//偽ライセンス鍵Kc//偽アクセス制御情報ACm//偽再生制御情報ACp）を受取り（ステップS584）。

【0209】そうすると、コントローラ510は、貸出先であるメモリカード110のライセンス管理情報から返却するライセンスが格納されているエントリ番号を取得し、その取得したエントリ番号を貸出先に送信する（ステップS586）。メモリカード110のコントローラ1420は、偽アクセス制御ACmによってライセンスの貸出が可能か否かを判定し（ステップS588）、貸出可であればライセンス領域の貸出フラグを「可」に設定し（ステップS590）、貸出不可であれば貸出フラグを「不可」に設定する（ステップS592）。ステップS590またはステップS592の後、コントローラ1420は、エントリ番号によって指定されたライセンス領域1415Aの有効フラグを「有効」に設定し（ステップS694）、エントリ番号によって指定された領域にライセンス（ライセンスID、コンテンツID、ライセンス鍵Kc、アクセス制御情報、および再生回数制御情報）を格納する（ステップS596）。ステップS588、S590、S592、S594、S596の処理は、上述した「配信」および「移動」と共通としているため、処理されるものの偽アクセス制御情報ACmは、常に移動複製禁止であるためステップS588においては必ず「貸出不可」と判断され、ステップS592に進む。

【0210】その後、コントローラ510は、ライセンスの検索要求を貸出先に再び入力し（ステップS598）、メモリカード110のコントローラ1420は、ライセンスの検索結果を端子1426、インタフェース1424、およびバスBS4を介して受取り（ステップS600）。コントローラ1420は、ライセンスIDに基づいてメモリ1415のライセンス領域1415Aを検索する。そして、コントローラ1420は、検索結果stateを生成する（ステップS602）。

【0211】暗号化処理部1406は、復号処理部1412によって復号して得られたセッションキーKs2aをスイッチ1442の接点Pbを介して受け、セッションキー発生部1418が発生したセッションキーKs2bをスイッチ1446の接点Pdを介して受ける。そして、暗号化処理部1406は、セッションキーKs2bをセッションキーKs2aによって暗号化して暗号化データ {Ks2b} Ks2aを生成する（ステップS604）。そして、コントローラ1420は、ライセンスID// {Ks2b} Ks2a//stateを生成し、

その生成したライセンスID// {Ks2b} Ks2a //stateのハッシュ値hashを求める(ステップS606)。つまり、コントローラ1420は、ライセンスID// {Ks2b} Ks2a//stateの署名を行なう。その後、コントローラ1420は、ハッシュ値hashをスイッチ1446の接点Pfを介して暗号化処理部1406へ与える。暗号化処理部1406は、ハッシュ値hashをセッションキーKs2aによって暗号化し、暗号化データ {hash} Ks2aを生成する(ステップS608)。

【0212】図21を参照して、メモリカード110のコントローラ1420は、ライセンスID// {Ks2b} Ks2a//state// {hash} Ks2aを生成し、バスBS4、インタフェース1424、および端子1426を介してライセンスID// {Ks2b} Ks2a//state// {hash} Ks2aを出力する(ステップS610)。コントローラ510は、端子580、USBインタフェース550を介してメモリカード110からライセンスID// {Ks2b} Ks2a//state// {hash} Ks2aを受信する(ステップS612)。そして、コントローラ510は、ライセンスID// {Ks2b} Ks2a//state// {hash} Ks2aとエントリ番号を指定したライセンス返却確認要求とをバスBS2を介して貸出元であるライセンス管理デバイス520へ入力する(ステップS614)。

【0213】ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224およびバスBS2を介してライセンスID// {Ks2b} Ks2a//state// {hash} Ks2aとエントリ番号とライセンス返却確認要求とを受信する(ステップS616)。そして、コントローラ5220は、受信したライセンスIDが貸出時のライセンスIDに一致するか否かを判定し(ステップS618)、不一致であれば返却動作は終了する(ステップS638)。そして、ステップS618において、2つのライセンスIDが一致すると判定されたとき、コントローラ5220は、メモリカード110におけるライセンスの検索結果stateを確認する(ステップS620)。すなわち、コントローラ5220は、返却しようとするライセンスがメモリカード110のライセンス領域1415Aから本当に消去されているか否かを確認し、ライセンス領域1415Aにライセンスが存在するとき、返却動作を終了する(ステップS638)。そして、コントローラ5220は、返却しようとするライセンスがメモリカード110のライセンス領域1415Aから消去されていることを確認したとき、ライセンスID// {Ks2b} Ks2a//stateのハッシュ値hashを求める(ステップS622)。つまり、ライセンス管理デバイス520のコントローラ5220は、自ら

ライセンスID// {Ks2b} Ks2a//stateに対する署名を行ない、ハッシュ値hashを求める。

【0214】その後、コントローラ5220は、ステップS554において受理した {hash} Ks2aを復号処理部5212に与える。復号処理部5212は、

{hash} Ks2aをセッションキーKs2aによって復号し、コントローラ5220は、メモリカード110におけるハッシュ値hashを受信する(ステップS624)。そして、コントローラ5220は、自ら求めたハッシュ値hashがメモリカード110におけるハッシュ値hashに一致するか否かを判定し(ステップS626)、不一致であるとき、メモリカード110における署名が書換えられていることになるので返却動作は終了する(ステップS638)。2つのハッシュ値が一致したとき、コントローラ5220は、ステップS616において受理した暗号化データ {Ks2b} Ks2aを復号処理部5212に与える。復号処理部5212は、暗号化データ {Ks2b} Ks2aをセッションキーKs2aによって復号してセッションキーKs2bを受信する(ステップS628)。

【0215】そして、コントローラ5220は、セッションキーKs2bの確認を行ない(ステップS630)、ライセンスの貸出時にメモリカード110から受信したセッションキーKs2bと不一致であれば返却動作は終了する(ステップS638)。ステップS630において2つのセッションキーKs2bが一致したとき、コントローラ1420は、エントリ番号によって指定されたエントリ内の貸出フラグを「可」に変更する(ステップS632)。そして、コントローラ40は、返却したライセンスの情報を削除し、貸出先のメモリカード110のデータ領域1415Bに記録されているライセンス管理情報および再生リストファイルを更新し、返却動作が終了する(ステップS638)。

【0216】このように、暗号化コンテンツデータおよびライセンスを貸出した相手先から暗号化コンテンツデータおよびライセンスを返却して貰うことによって、ライセンス管理デバイス520にライセンスを残したまま、携帯電話機100および再生端末102において暗号化コンテンツデータを再生して楽しむことができる。

【0217】また、メモリカードへ貸出されたライセンスは、アクセス制御情報AcMによってメモリカードから他の記録機器(メモリカード、ライセンス管理デバイスおよびライセンス管理モジュール)に対して、チェックアウトしたライセンスが出力できないよう指定されているため、貸出したライセンスが流出することはない。貸出したライセンス管理モジュールに対してチェックイン(返却)することで、貸出したライセンスの権利が、貸出したライセンス管理デバイスに戻るようになっている。したがって、著作者の意に反して複製ができること

を許すものではなく、セキュリティレベルが低下する処理ではなく、著作権も保護されている。

【0218】図22を参照して、パーソナルコンピュータ50のライセンス管理モジュール511またはライセンス管理デバイス520によって受信された暗号化コンテンツデータおよびライセンスの管理について説明する。パーソナルコンピュータ50のHDD530は、コンテンツリストファイル150と、コンテンツファイル1531~1535と、ライセンス管理ファイル1521~1525とを含む。

【0219】コンテンツリストファイル150は、所有するコンテンツの一覧形式のデータファイルであり、個々のコンテンツに対する情報（楽曲名、アーティスト名など）と、コンテンツファイルとライセンス管理ファイルとを示す情報（ファイル名）などが含まれている。個々のコンテンツに対する情報は受信時に付加情報Dc-infから必要な情報を取得して自動的に、あるいは、ユーザの指示によって記載される。また、コンテンツファイルのみ、ライセンス管理ファイルのみの再生できないコンテンツについても一覧の中で管理することが可能である。

【0220】コンテンツファイル1531~1535は、ライセンス管理モジュール511またはライセンス管理デバイス520によって受信された暗号化コンテンツデータ {Dc} Kcと付加情報Dc-infとを記録するファイルであり、コンテンツごとに設けられる。

【0221】また、ライセンス管理ファイル1521~1525は、それぞれ、コンテンツファイル1531~1535に対応して記録されており、ライセンス管理モジュール511またはライセンス管理デバイス520によって受信されたライセンスを管理するためのファイルである。これまでの説明でも明らかなように、ライセンスは通常参照することができないが、ライセンス鍵Kcを除く他の情報は、ユーザが書き換えることさえできなければ著作権保護の点では問題ない。しかし、運用においてライセンス鍵Kcと分離して管理することはセキュリティの低下につながるため好ましくない。そこで、ライセンス配信を受ける場合に平文にて参照できるトランザクションID、コンテンツIDや、ライセンス購入条件ACから容易に判断できるアクセス制御情報ACmおよび再生制御情報ACPにて制限されている事項の写しおよびチェックアウトの記録を平文にて記録する。さらに、ライセンス管理デバイス520にライセンスが記録された場合にはエントリ番号を記録する。

【0222】ライセンス管理ファイル1521、1522、1524、1525は、それぞれ、エントリ番号0、2、1、3を含む。これは、ライセンス管理デバイス520によって受信され、ライセンス管理デバイス520のメモリ5215のライセンス領域5215Aにおいて管理されるライセンス（ライセンスID、ライセン

ス鍵Kc、アクセス制御情報ACmおよび再生制御情報ACm)の管理領域を指定する番号である。

【0223】また、コンテンツファイル1531に記録されたファイル名の暗号化コンテンツデータを携帯電話機100または再生端末102に装着されたメモリカード110へ移動させるとき、コンテンツファイル1531~1535を検索してコンテンツファイル1531を抽出すれば、暗号化コンテンツデータを再生するライセンスがどこで管理されているかが解かる。コンテンツファイル1531に対応するライセンス管理ファイル1521に含まれるエントリ番号は「0」であるので、コンテンツファイル1531に記録されたファイル名の暗号化コンテンツデータを再生するライセンスは、ライセンス管理デバイス520のメモリ5215のライセンス領域5215Aのエントリ番号0によって指定された領域に記録されている。そうすると、HDD530に記録されたコンテンツリストファイル150のライセンス管理ファイル1521からエントリ番号0を読み出し、その読出したエントリ番号0をライセンス管理デバイス520に入力することによって、メモリ5215のライセンス領域5215Aからライセンスを容易に取出し、メモリカード110へ移動できる。そして、ライセンスを移動した後は、メモリ5215のライセンス領域5215Aにおいて指定されたエントリ番号内の有効フラグが「無効」にされるので（図15のステップS346参照）、それに対応してライセンス管理ファイル1523のように「ライセンス無」が記録される。

【0224】ライセンス管理ファイル1523は、「ライセンス無」を含む。これは、ライセンス管理デバイス520によって受信されたライセンスが、移動された結果である。対応するコンテンツファイル1533はHDD530に記録されたままになっている。メモリカードからライセンスを再びライセンス管理モジュール520へ移動、あるいは、配信サーバ10から再び配信を受ける場合には、ライセンスについてのみ配信を受けることが可能である。

【0225】貸出および返却においても、同様にエントリ番号を指定して処理することができる。また、貸出においては、ライセンス管理ファイルは、貸出の有無および貸出先を特定するための情報、たとえば、メモリカードに割当てられたメディアID等および貸出時のライセンスIDを記録する。これらの情報は、返却時に消去される。

【0226】このように、本発明においては、ライセンス管理デバイス520に記録されているライセンスをライセンス管理デバイス520に残したまま、セキュリティレベルを低下させることなく、著作権を保護しながら暗号化コンテンツデータの再生を携帯電話機100や再生端末102によって自由に行なうことができる。

【0227】図23は、メモリカード110のメモリ1

10

20

30

40

50

415におけるライセンス領域1415Aとデータ領域1415Bとを示したものである。データ領域1415Bには、再生リストファイル160とコンテンツファイル1611~161nと、ライセンス管理ファイル1621~162nとが記録されている。コンテンツファイル1611~161nは、受信した暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infとを1つのファイルとして記録する。また、ライセンス管理ファイル1621~162nは、それぞれ、コンテンツファイル1611~161nに対応して記録されている。パーソナルコンピュータ50におけるHDD530に記録されていた各データがメモリカード110のメモリ1415のデータ領域1415Bに記録されているのみで、他の点は、図22と同じである。

【0228】また、ライセンス管理ファイル1622は、点線で示されているが、実際には記録されていないことを示す。コンテンツファイル1612は存在しているがライセンスが無く再生できないことを表しているが、これは、たとえば、再生端末が他の携帯電話機から暗号化コンテンツデータだけを受信した場合に相当する。

【0229】また、コンテンツファイル1613は、点線で示されているが、これは、たとえば、再生端末が配信サーバ10から暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータだけをパーソナルコンピュータ50へ送信した場合に相当し、ライセンスはメモリ1415に存在するが暗号化コンテンツデータが存在しないことを意味する。

【0230】なお、ライセンス管理領域1415Aは、ライセンス管理デバイスのライセンス管理領域5215Aと同じ構成になっている。したがって、メモリカード110から他のメモリカードへの貸出し、さらにはライセンス管理デバイス520への貸出しも可能である。

【0231】〔再生〕上述したように、携帯電話機100または再生端末102に装着されたメモリカード110は、配信サーバ10から、直接、暗号化コンテンツデータおよびライセンスを受信できる。また、メモリカード110は、パーソナルコンピュータ50が配信サーバ10からハード的に取得した暗号化コンテンツデータおよびライセンスを、「移動」という概念によってパーソナルコンピュータ50から受信できる。さらに、メモリカード110は、パーソナルコンピュータ50が配信サーバ10または音楽CDからソフト的に取得した暗号化コンテンツデータおよびライセンスを、「貸出」という概念によってパーソナルコンピュータ50から受信できる。

【0232】このように、メモリカード110は、各種の方法によって暗号化コンテンツデータおよびライセンスを受信する。そこで、次に、これらの各種の方法によってメモリカードが受信した暗号化コンテンツデータの

再生について説明する。

【0233】図24は、メモリカード110が受信したコンテンツデータの再生端末102における再生動作を説明するためのフローチャートである。なお、図24における処理以前に、再生端末102のユーザは、メモリカード100のデータ領域1415Bに記録されている再生リストに従って、再生するコンテンツ(楽曲)を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提として説明する。

【0234】図24を参照して、再生動作の開始とともに、再生端末100のユーザから操作パネル1108を介して再生リクエストが再生端末100にインプットされる(ステップS700)。そうすると、コントローラ1106は、バスBS3を介して認証データの出力要求をコンテンツ再生回路1550に行ない(ステップS702)、コンテンツ再生回路1550は認証データの出力要求を受信する(ステップS704)。そして、認証データ保持部1500は、認証データ{Kpp1//Cp1}KPaを出力し(ステップS706)、コントローラ1106は、メモリカードインタフェース1200を介してメモリカード110へ認証データ{Kpp1//Cp1}KPaを入力する(ステップS708)。

【0235】そうすると、メモリカード110は、認証データ{Kpp1//Cp1}KPaを受信し、復号処理部1408は、受信した認証データ{Kpp1//Cp1}KPaを、KPa保持部1414に保持された公開認証鍵KPaによって復号し(ステップS710)、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ{Kpp1//Cp1}KPaが正規の認証データであるか否かを判断する認証処理を行なう(ステップS712)。復号できなかった場合、ステップS748へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ1420は、セッションキー発生部1418を制御し、セッションキー発生部1418は、再生セッション用のセッションキーKs2を発生させる(ステップS714)。そして、暗号処理部1410は、セッションキー発生部1418からのセッションキーKs2を、復号処理部1408で復号された公開暗号鍵Kpp1によって暗号化した{Ks2}Kp1をバスBS3へ出力する。そうすると、コントローラ1420は、インタフェース1424および端子1426を介してメモリカードインタフェース1200へ{Ks2}Kp1を出力する(ステップS716)。再生端末100のコントローラ1106は、メモリカードインタフェース1200を介して{Ks2}Kp1を取得する。そして、コントローラ1106は、{Ks2}Kp1をバスBS3を介してコンテンツ再生回路1550の復号処理部1504へ与え(ステップS718)、復号処理部1504は、Kp1保持部1502から出力された、公開

暗号鍵K P p 1と対になっている秘密復号鍵K p 1によって{K s 2} K p 1を復号し、セッションキーK s 2を暗号処理部1506へ出力する(ステップS 720)。そうすると、セッションキー発生部1508は、再生セッション用のセッションキーK s 3を発生させ、セッションキーK s 3を暗号処理部1506へ出力する(ステップS 722)。暗号処理部1506は、セッションキー発生部1508からのセッションキーK s 3を復号処理部1504からのセッションキーK s 2によって暗号化して{K s 3} K s 2を出力し(ステップS 724)、コントローラ1106は、バスBS 3およびメモリカードインタフェース1200を介して{K s 3} K s 2をメモリカード110へ出力する(ステップS 726)。

【0236】そうすると、メモリカード110の復号処理部1412は、端子1426、インタフェース1424、およびバスBS 4を介して{K s 3} K s 2を入力する。復号処理部1412は、セッションキー発生部1418によって発生されたセッションキーK s 2によって{K s 3} K s 2を復号して、再生端末100で発生されたセッションキーK s 3を受理する(ステップS 728)。

【0237】再生端末のコントローラ1106は、メモリカード110から事前に取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し(ステップS 730)、メモリカードインタフェース1200を介してメモリカード110へ取得したエントリ番号とライセンスの出力要求を出力する(ステップS 732)。

【0238】メモリカード110のコントローラ1420は、エントリ番号とライセンスの出力要求とを受理し、エントリ番号によって指定された領域に格納されたライセンスを取得する(ステップS 734)。

【0239】そして、コントローラ1420は、アクセス制限情報AC mを確認する(ステップS 736)。

【0240】ステップS 736においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報AC mを確認することにより、具体的には、再生回数を確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に制限がある場合にはアクセス制限情報AC mの再生回数を変更した(ステップS 738)後に次のステップ(ステップS 740)に進む。一方、アクセス制限情報AC mの再生回数によって再生が制限されていない場合には、ステップS 738はスキップされ、アクセス制限情報AC mの再生回数は変更されることなく処理が次のステップ(ステップS 740)に進行される。

【0241】ステップS 736において、当該再生動作において再生が可能であると判断された場合には、メモリ1415のライセンス領域1415Aに記録された再

生リクエスト曲のライセンス鍵K cおよび再生制御情報AC pがバスBS 4上に出力される(ステップS 740)。

【0242】得られたライセンス鍵K cと再生制御情報AC pは、切換スイッチ1446の接点P fを介して暗号化処理部1406に送られる。暗号化処理部1406は、切換スイッチ1442の接点P bを介して復号処理部1412より受けたセッションキーK s 3によって切換スイッチ1446を介して受けたライセンス鍵K cと再生制御情報AC pとを暗号化し、{K c//AC p} K s 3をバスBS 4に出力する(ステップS 740)。

【0243】バスBS 4に出力された暗号化データは、インタフェース1424、端子1426、およびメモリカードインタフェース1200を介して再生端末102に送出される。

【0244】再生端末102においては、メモリカードインタフェース1200を介してバスBS 3に伝達される暗号化データ{K c//AC p} K s 3を復号処理部1510によって復号処理を行ない、ライセンス鍵K cおよび再生制御情報AC pを受理する(ステップS 742, S 744)。復号処理部1510は、ライセンス鍵K cを復号処理部1516に伝達し、再生制御情報AC pをバスBS 3に出力する。

【0245】コントローラ1106は、バスBS 3を介して、再生制御情報AC pを受理して再生の可否の確認を行なう(ステップS 746)。

【0246】ステップS 746においては、再生制御情報AC pによって再生不可と判断される場合には、再生動作は終了される。

【0247】ステップS 746において再生可能と判断された場合、コントローラ1106は、メモリカードインタフェース1200を介してメモリカード110に暗号化コンテンツデータ{D c} K cを要求する。そうすると、メモリカード110のコントローラ1420は、メモリ1415から暗号化コンテンツデータ{D c} K cを取得し、バスBS 4、インタフェース1424、および端子1426を介してメモリカードインタフェース1200へ出力する。

【0248】再生端末102のコントローラ1106は、メモリカードインタフェース1200を介して暗号化コンテンツデータ{D c} K cを取得し、バスBS 3を介して暗号化コンテンツデータ{D c} K cをコンテンツ再生回路1550へ与える。

【0249】そして、コンテンツ再生回路1550の復号処理部1516は、暗号化コンテンツデータ{D c} K cを復号処理部1510から出力されたライセンス鍵K cによって復号してコンテンツデータD cを取得する。

【0250】そして、復号されたコンテンツデータD cは音楽再生部1518へ出力され、音楽再生部1518

10

20

30

40

50

は、コンテンツデータを再生し、DA変換器1519はデジタル信号をアナログ信号に変換して端子1530へ出力する。そして、音楽データは端子1530から外部出力装置を介してヘッドホン130へ出力されて再生される。これによって再生動作が終了する(ステップS748)。

【0251】本発明の実施の形態によれば、貸出元のメモリカードは、貸出したライセンスを貸出先IDおよび貸出時ライセンスIDによって管理し、ライセンスの貸出を貸出フラグによって管理し、ライセンスの貸出時に貸出用ライセンスを自己が保持したライセンスから生成し、元のライセンスが貸出中であることを示すフラグを貸出フラグに設定するので、貸出したライセンスのバックアップを提供することができる。

【0252】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【0253】

【発明の効果】本発明によれば、貸出元のメモリカードは、貸出したライセンスを貸出先IDおよび貸出時ライセンスIDによって管理し、ライセンスの貸出を貸出フラグによって管理し、ライセンスの貸出時に貸出用ライセンスを自己が保持したライセンスから生成し、元のライセンスが貸出中であることを示すフラグを貸出フラグに設定するので、貸出したライセンスのバックアップを提供することができる。

【図面の簡単な説明】

【図1】 データ配信システムを概念的に説明する概略図である。

【図2】 他のデータ配信システムを概念的に説明する概略図である。

【図3】 図1および図2に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図4】 図1および図2に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図5】 図1および図2に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図6】 図1および図2に示すデータ配信システムにおけるパーソナルコンピュータの構成を示す概略ブロック図である。

【図7】 図2に示すデータ配信システムにおける再生端末の構成を示す概略ブロック図である。

【図8】 図1および図2に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図9】 図6に示すライセンス管理デバイスの構成を示す概略ブロック図である。

【図10】 図1および図2に示すデータ配信システムにおける配信動作を説明するための第1のフローチャートである。

【図11】 図1および図2に示すデータ配信システムにおける配信動作を説明するための第2のフローチャートである。

【図12】 リッピングを実行するソフトウェアの機能を説明するための機能ブロック図である。

【図13】 図1および図2に示すデータ配信システムにおけるリッピングの動作を説明するためのフローチャートである。

【図14】 図1および図2に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第1のフローチャートである。

【図15】 図1および図2に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第2のフローチャートである。

【図16】 図1および図2に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの貸出動作を説明するための第1のフローチャートである。

【図17】 図1および図2に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの貸出動作を説明するための第2のフローチャートである。

【図18】 図1および図2に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの返却動作を説明するための第1のフローチャートである。

【図19】 図1および図2に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの返却動作を説明するための第2のフローチャートである。

【図20】 図1および図2に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの返却動作を説明するための第3のフローチャートである。

【図21】 図1および図2に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの返却動作を説明するための第4のフローチャートである。

【図22】 パーソナルコンピュータのハードディスクにおけるコンテンツリストファイルの構成を示す図である。

【図23】 メモリカードにおける再生リストファイルの構成を示す図である。

【図24】 再生端末における再生動作を説明するためのフローチャートである。

【符号の説明】

10 配信サーバ、20 配信キャリア、30 インターネット網、50 パーソナルコンピュータ、60 音楽CD、70 USBケーブル、100 携帯電話機、102 再生端末、110 メモリカード、130 ヘッドホン、150 コンテンツリストファイル、16

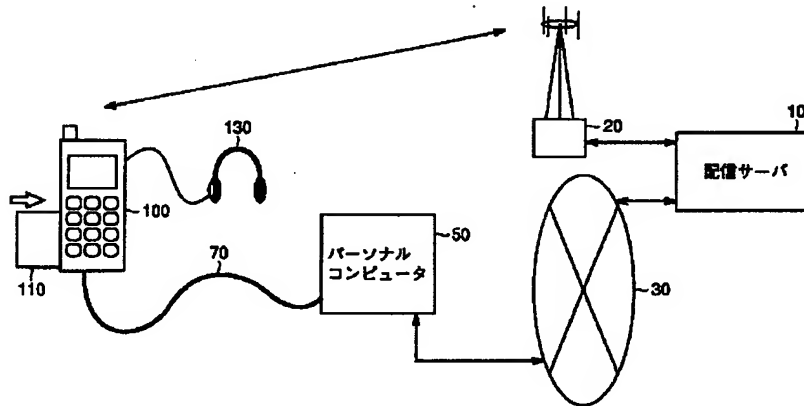
57

0 再生リストファイル、302 課金データベース、
304 情報データベース、307 メニューデータベ
ース、308 配信記録データベース、310 データ
処理部、312、320、1404、1408、141
2、1422、1504、1510、1516、520
4、5208、5212、5222 復号処理部、31
3 認証鍵保持部、315 配信制御部、316、セ
ッションキー発生部、318、326、328、140
6、1410、1417、1506、5206、521
0、5217、5405 暗号処理部、350 通信装
置、510、1106、1420、5220コントロー
ラ、520 ライセンス管理デバイス、530 ハード
ディスク、550、1112 USBインタフェース、
555 モデム、560 キーボード、570 ディス
プレイ、580、1114、1426、1530、52
26端子、1108 操作パネル、1110 表示パネ
ル、1200 メモリカードインタフェース、140 *

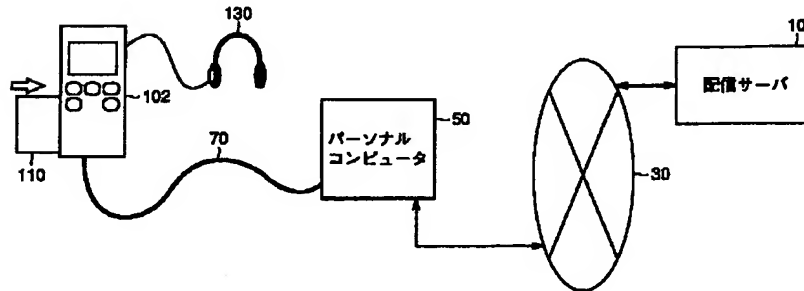
58

*0、1500、5200 認証データ保持部、140
2、5202 Kmc保持部、1414、5214 K
Pa保持部、1415、5215 メモリ、1415A
ライセンス領域、1415B データ領域、141
6、5216 KPmc保持部、1418、5218
セッションキー発生部、1421、5221 Km保持
部、1424、5224 インタフェース、1442、
1446、5242、5246 切換スイッチ、150
2 Kp1保持部、1518 音楽再生部、1519
DA変換器、1521~1525、1621~162n
ライセンス管理ファイル、1531~1535、16
11~161n コンテンツファイル、1550 コン
テンツ再生回路、5400 ウォータマーク検出手段、
5401 ウォータマーク判定手段、5402 リマー
ク手段、5403 ライセンス発生手段、5404 音
楽エンコーダ。

【図1】



【図2】



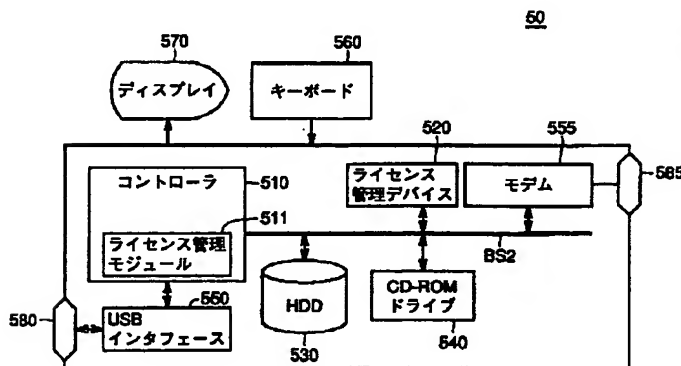
【図3】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、動画データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ (Dc)Kcとして配信され、メモリカードに保持される
Dc-Inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス 暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	ライセンスを特定するための管理コード
ライセンス	ライセンス	ライセンス固有	Kc+ACm+ACp+コンテンツID+ライセンスIDの総称
有効フラグ	フラグ	ライセンス固有	ライセンスをメモリカードから外部へ出すことが可能か否かを表す。
貸出フラグ	フラグ	ライセンス固有	ライセンスの貸出の可否を表す。
貸出先ID	特定情報	メモリカード固有	ライセンスを貸出した貸出先を特定するための情報
貸出時ライセンスID	識別情報	ライセンス固有	貸出したライセンスを識別するための情報

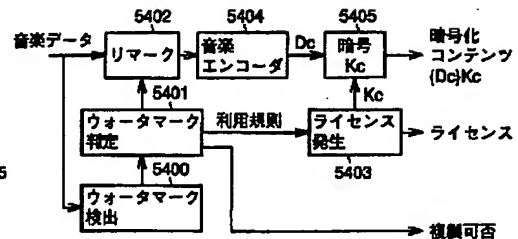
【図4】

記号	種類	属性	特性
配信サーバ	KPa	公開暗号鍵	システム共有 認証局にて認証データを復号する鍵
	Ka1	共通鍵	セッション固有 メモリカード、ライセンス管理デバイスへのライセンス配信ごとに発生
メモリカード	KPa	公開暗号鍵	システム共有 認証局にて認証データを復号する鍵 配信サーバのKPaと同一
ライセンス管理デバイス	KPmw	公開暗号鍵	クラス固有 証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
	Kmw	秘密復号鍵	クラス固有 公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な復号鍵
	KPmcx	公開暗号鍵	個別 メモリカードごとに異なる。 xはモジュールを識別するための識別子
	Kmcx	秘密復号鍵	個別 公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な復号鍵
	Ka2	共通鍵	セッション固有 ライセンスの授受ごとに発生
	Cmw	証明書	クラス証明書 メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書。署名機能を有する。 (KPmw/Cmw)KPaの形式で出荷時に配信。 *メモリカードおよびライセンス管理デバイスのクラスwごとに異なる。
コンテンツ再生回路	KPpy	公開暗号鍵	クラス固有 証明書Cmwとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
	Kpy	秘密復号鍵	クラス固有 公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ka3	共通鍵	セッション固有 配信サーバまたは音楽再生モジュール間の再生セッションごとに発生
	Cpy	証明書	クラス証明書 コンテンツ再生回路のクラス証明書。署名機能を有する。 (KPpy/Cpy)KPaの形式で出荷時に配信。 *コンテンツ再生回路のクラスyごとに異なる。

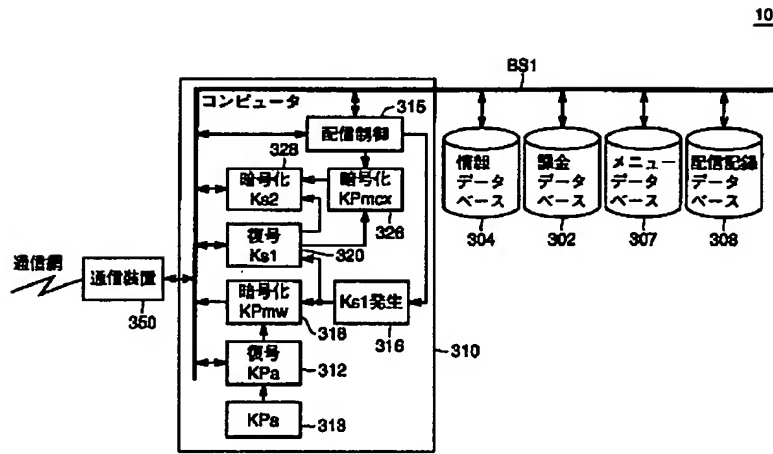
【図6】



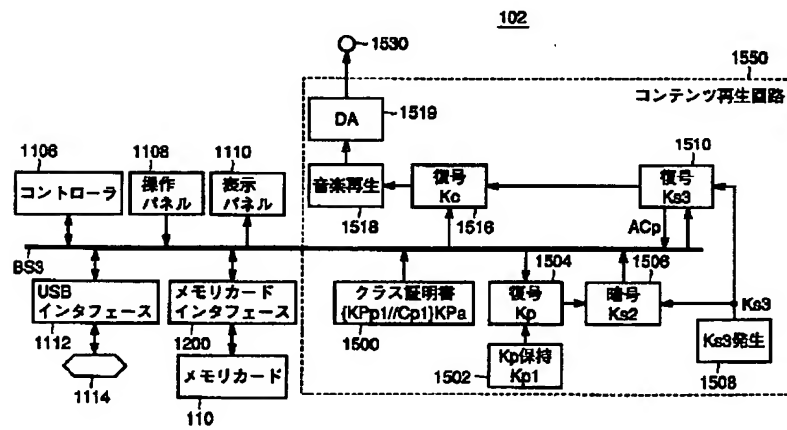
【図12】



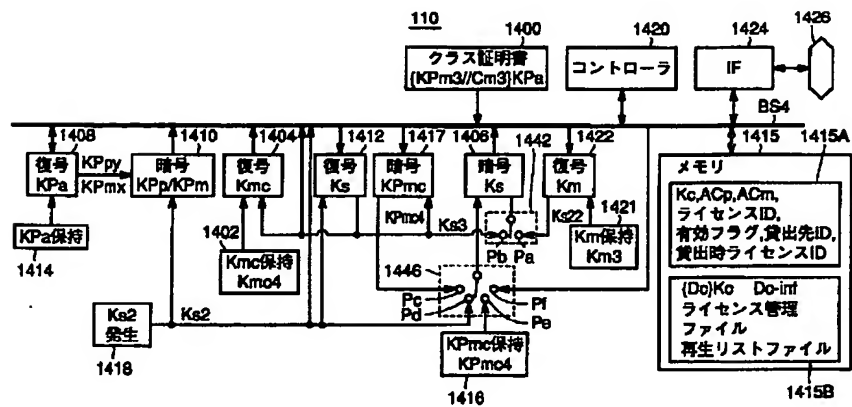
【図5】



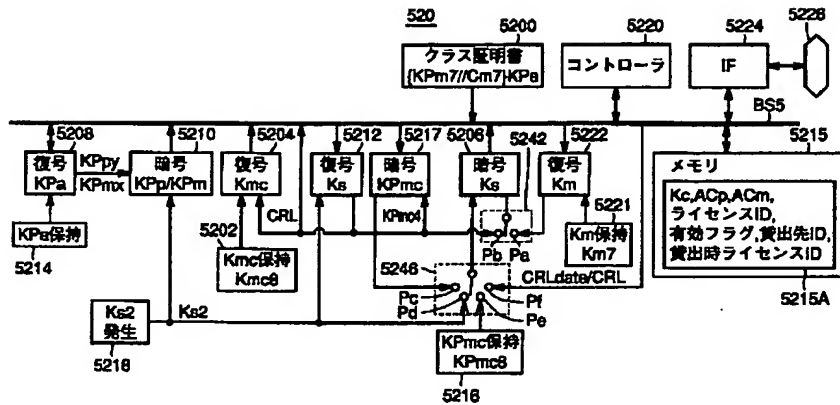
【図7】



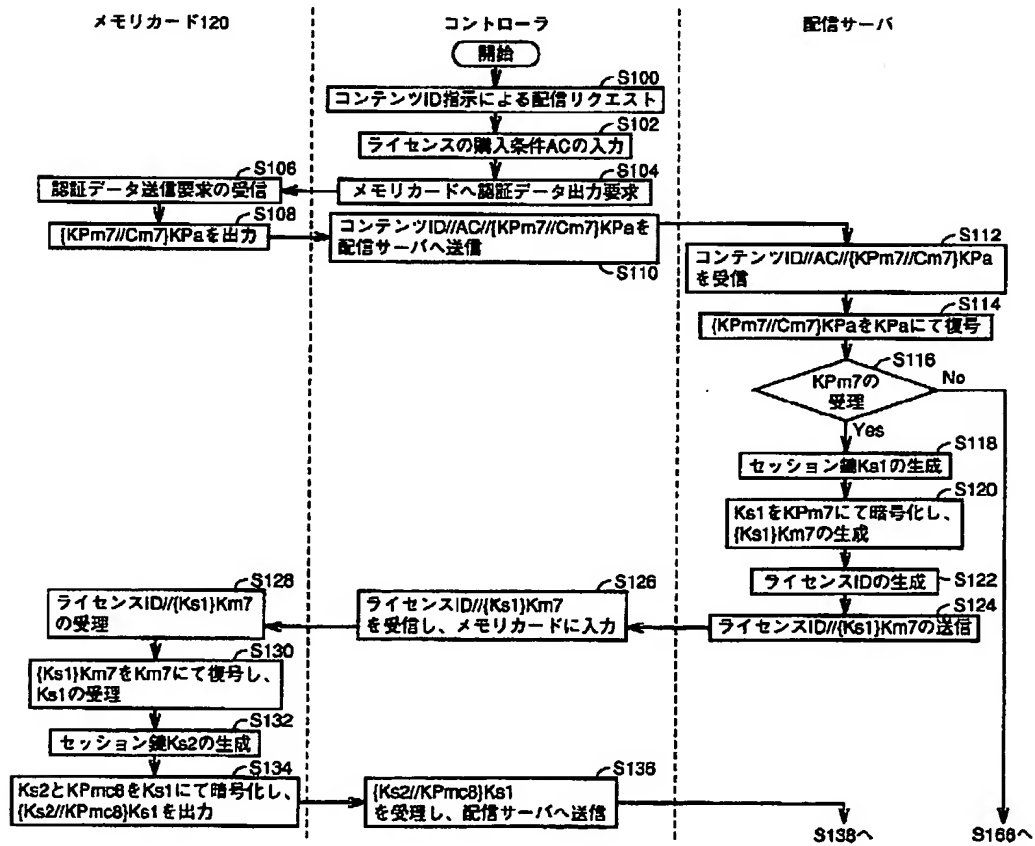
【図8】



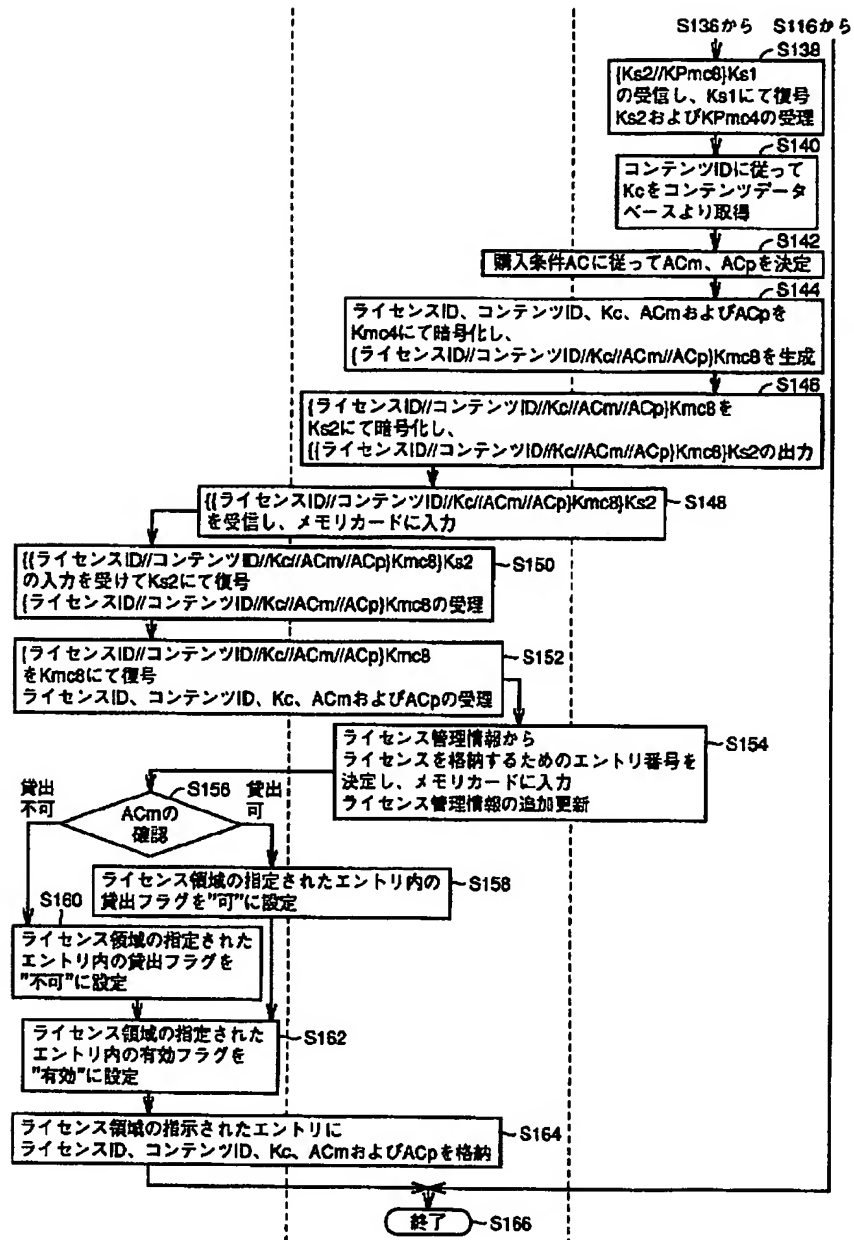
【図9】



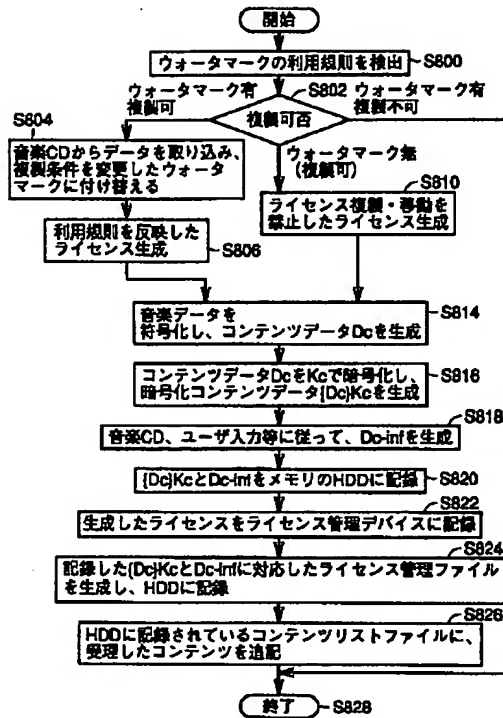
【図10】



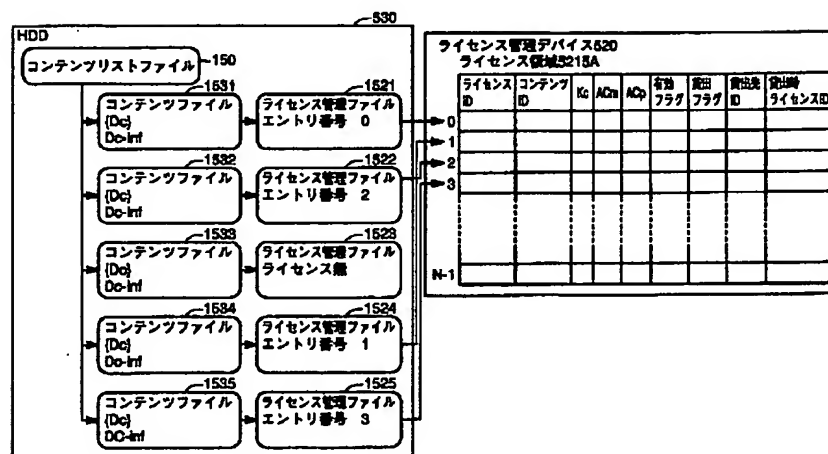
【図11】



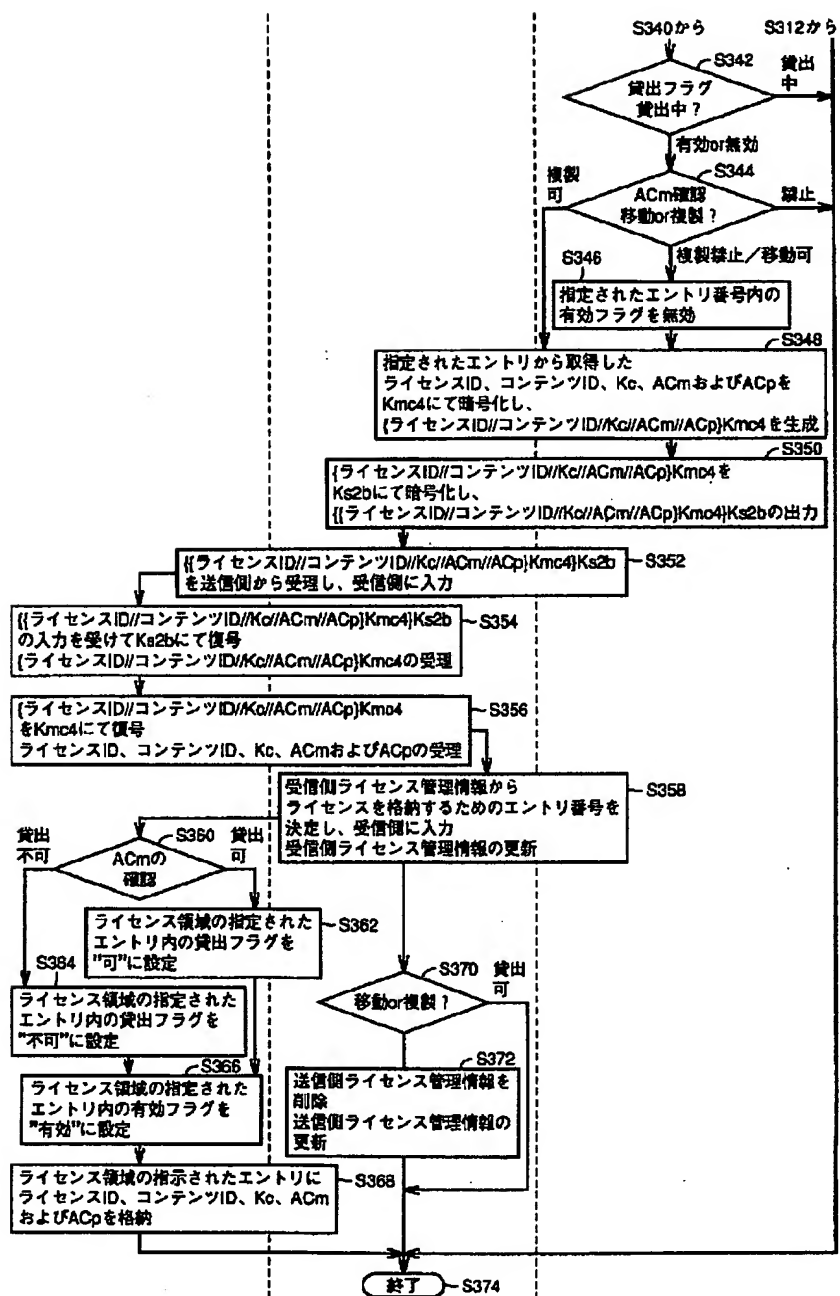
【図13】



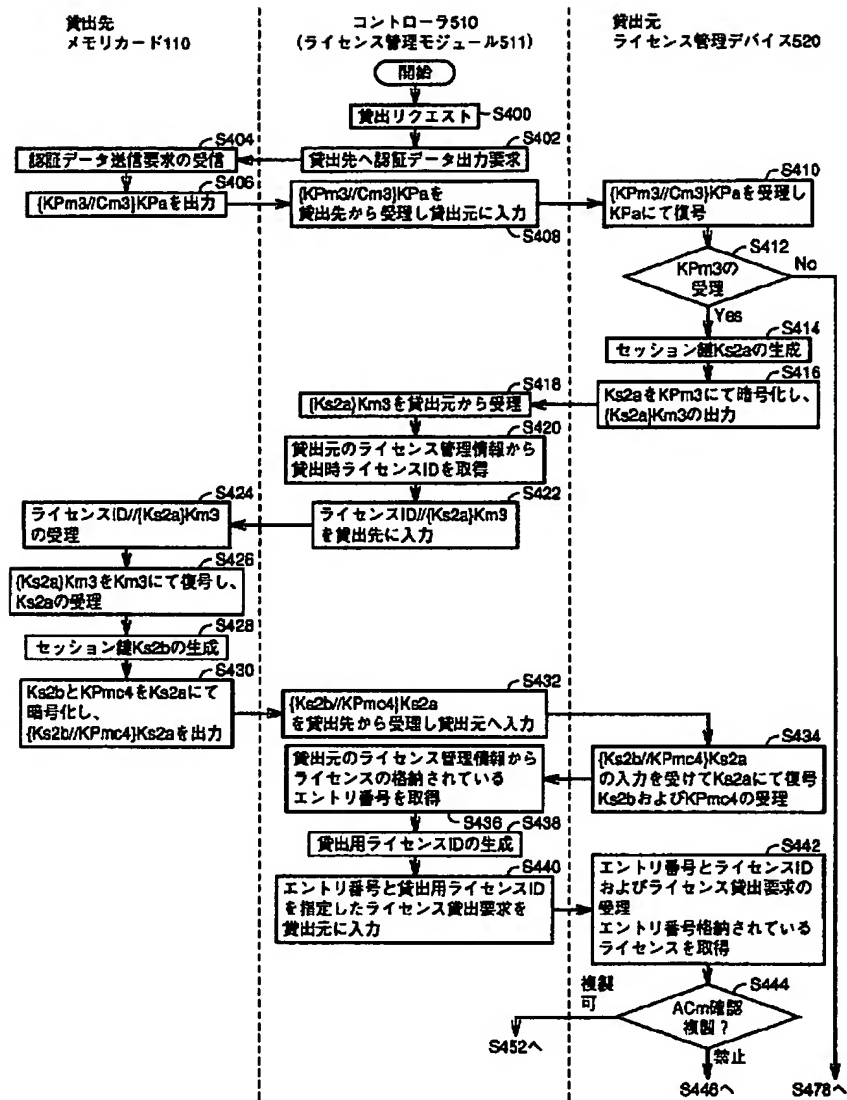
【図22】



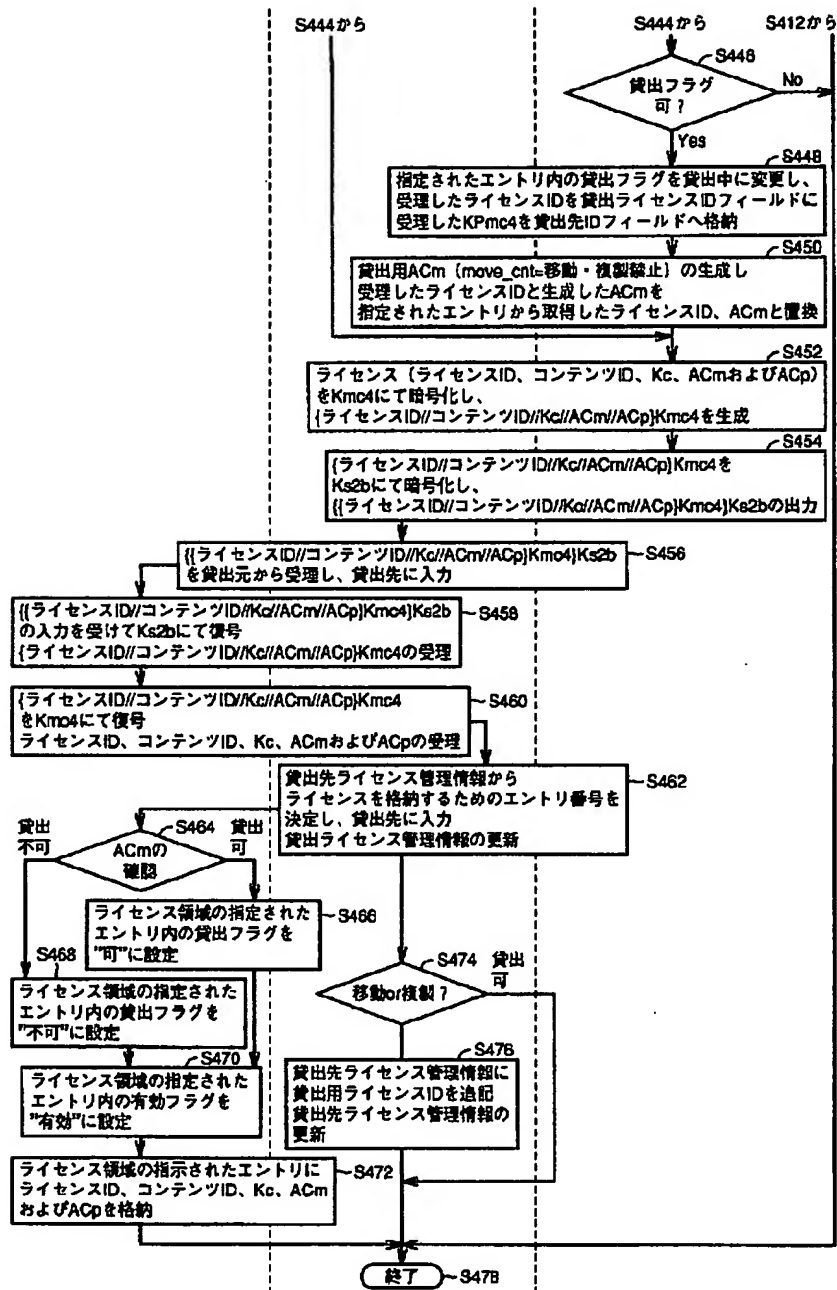
【図 15】



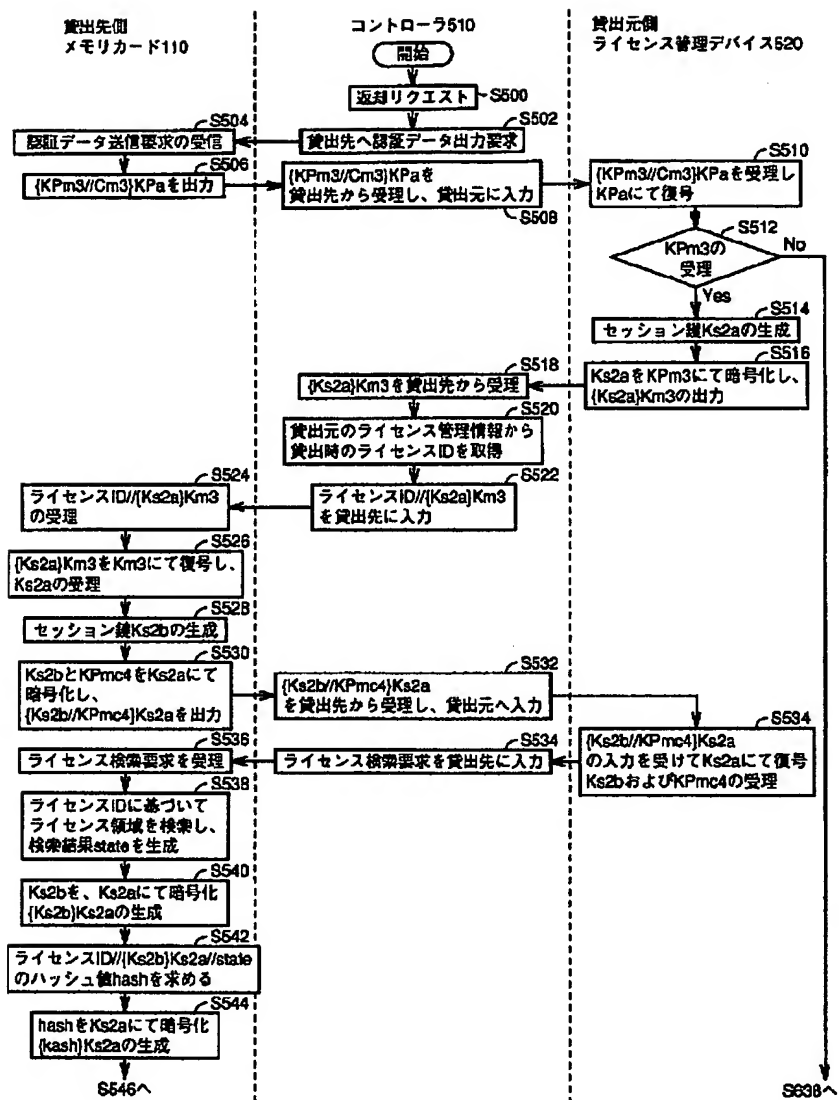
【図16】



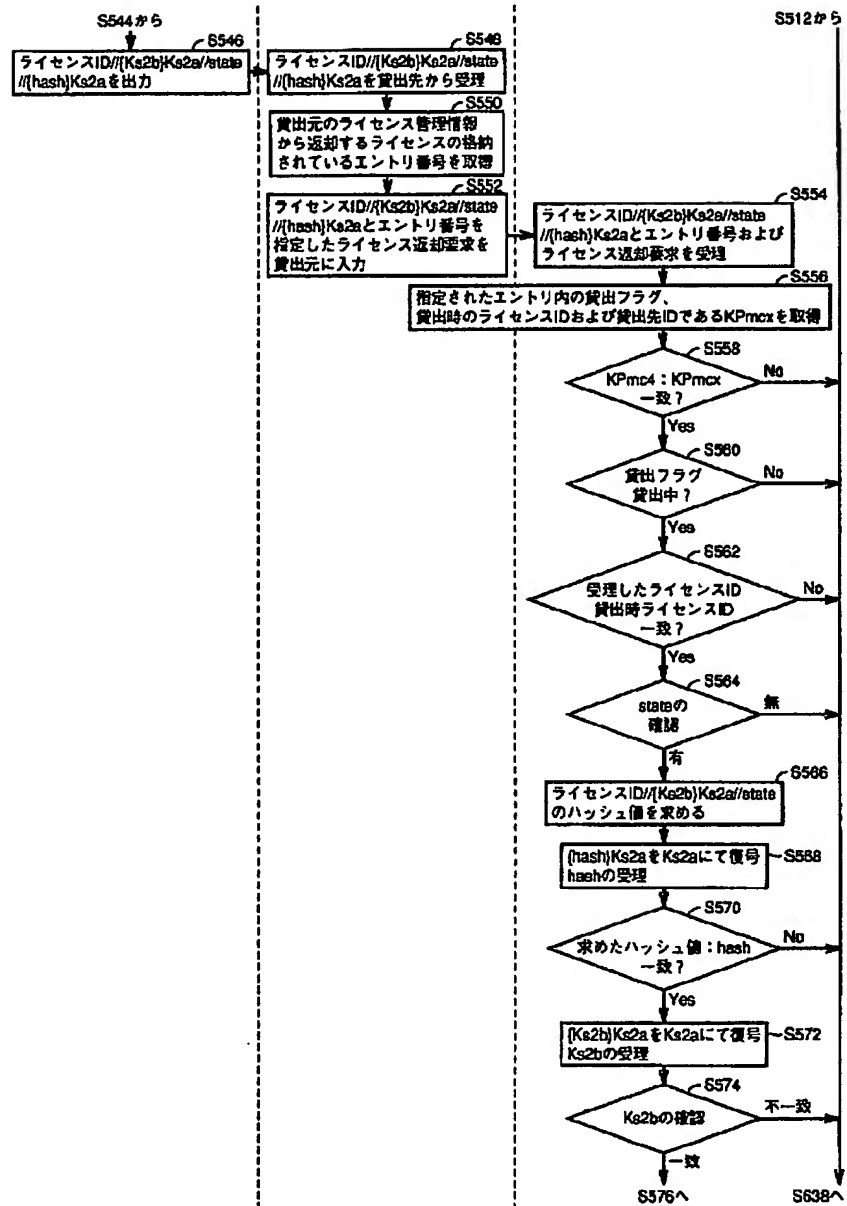
【図17】



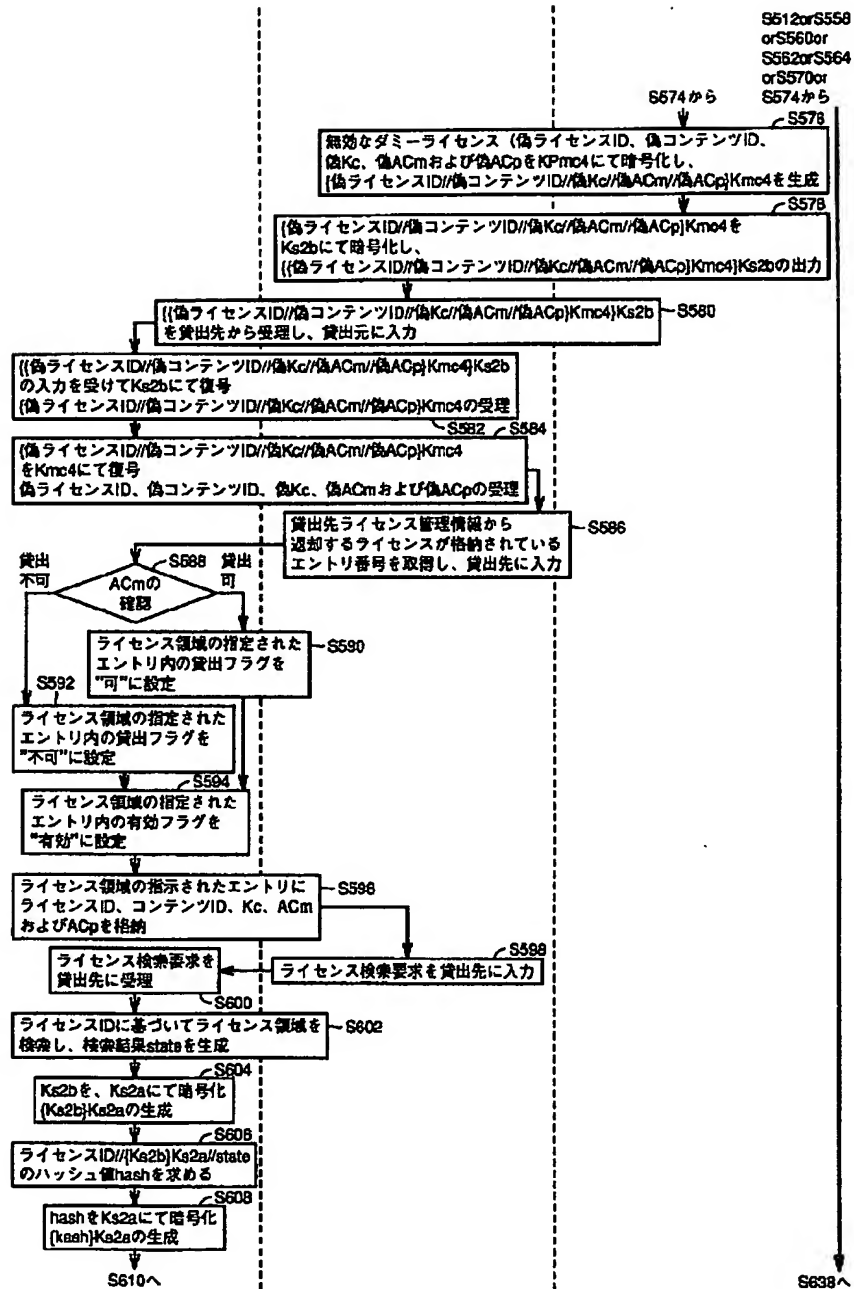
【図18】



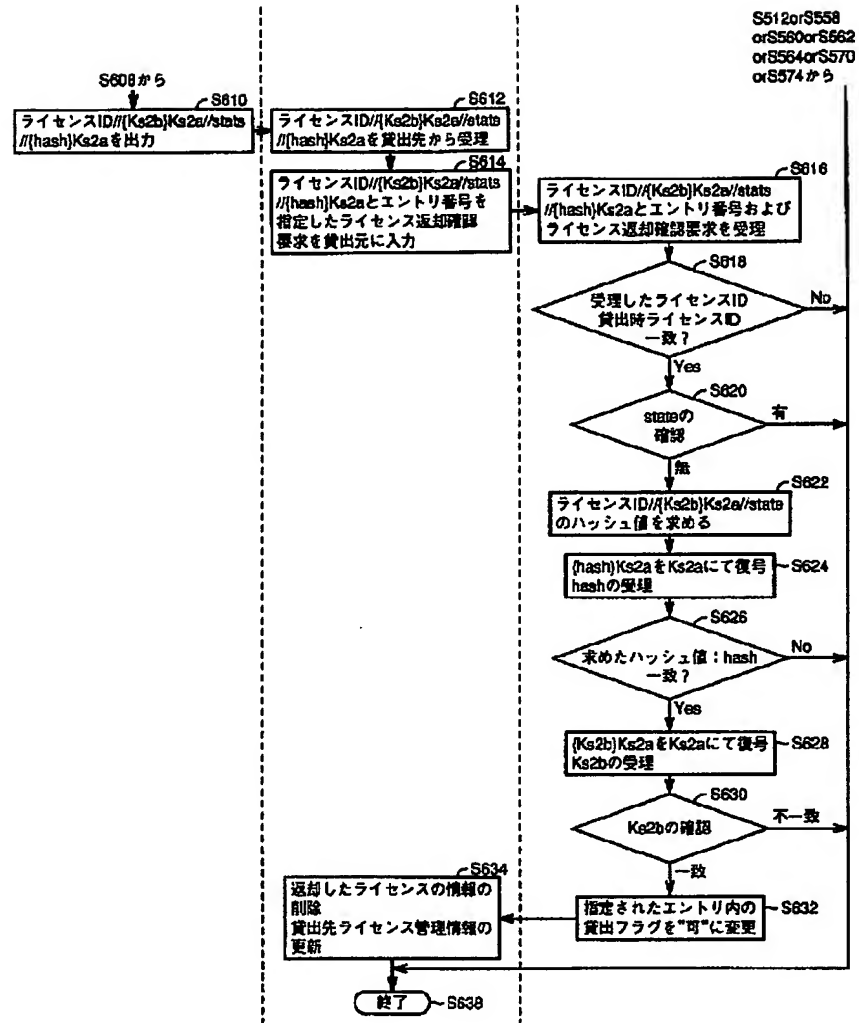
【図19】



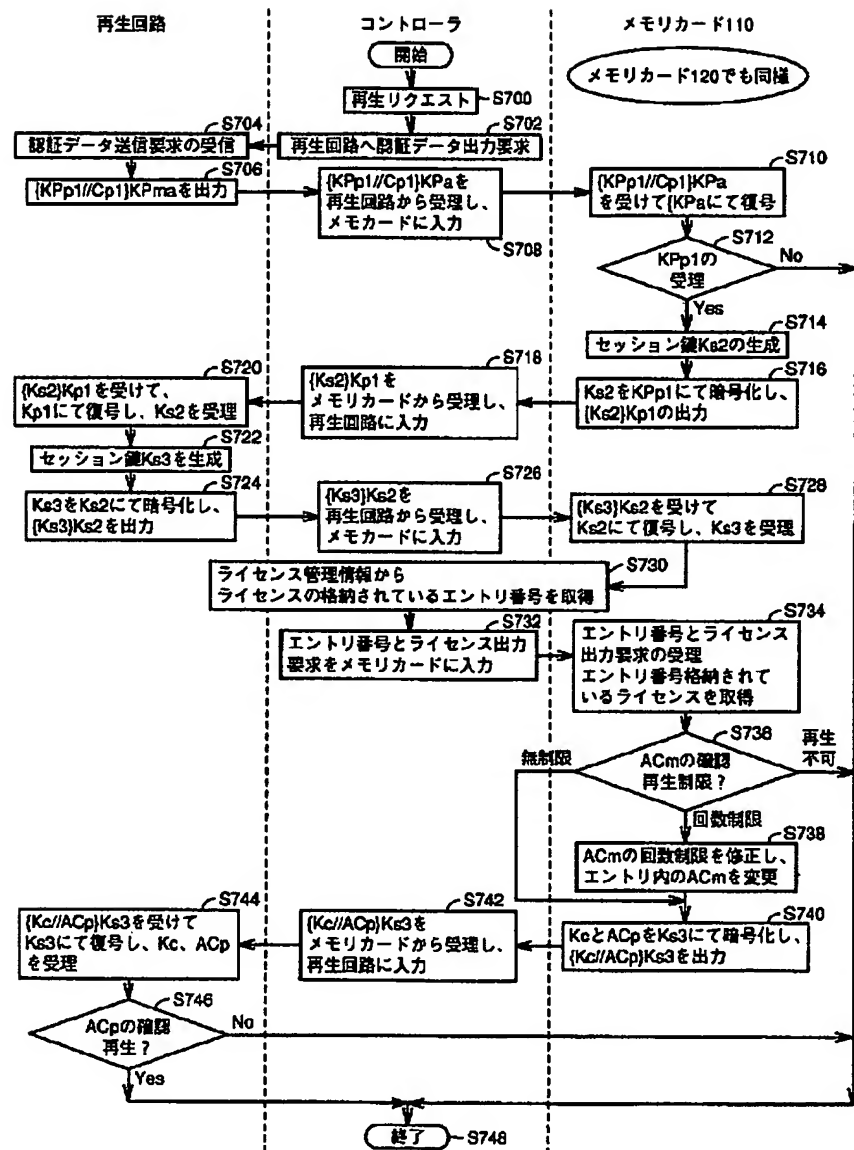
【図20】



【図21】



【図24】



フロントページの続き

(51)Int.Cl.⁷
G 0 6 K 19/07

識別記号

F I
G 0 6 K 19/00ターマード (参考)
N